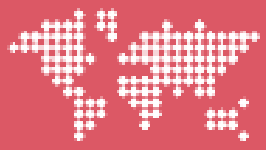
THEMATIC AUDIT

REVIEW OF ANTI-FRAUD PROGRAMME AT UN WOMEN



UN WOMEN

THEMATIC AUDIT

REVIEW OF ANTI-FRAUD PROGRAMME AT UN WOMEN

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

26 October 2021
IEAS/IAS/2021/006

UN WOMEN

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

ACRONYMS AND ABBREVIATIONS v

I. INTRODUCTION 1

II. BACKGROUND 1

III. AUDIT OBJECTIVES, SCOPE AND METHODOLOGY 3

IV. AUDIT RESULTS 6

A. OVERALL ASSESSMENT 6

B. FRAUD RISK GOVERNANCE 6

C. FRAUD RISK ASSESSMENTS 12

D. FRAUD POLICIES AND CONTROL ACTIVITIES 16

E. FRAUD INVESTIGATION AND CORRECTIVE ACTION 18

F. FRAUD MONITORING 21

V. RECOMMENDATIONS AND MANAGEMENT ACTION PLAN 23

ANNEX 1. DEFINITIONS OF AUDIT TERMS RATINGS AND PRIORITIES 28

EXECUTIVE SUMMARY

Audit objective and scope

During its annual risk assessment, the UN Women Internal Audit Service (IAS) of the Independent Evaluation and Audit Services (IEAS) selected UN Women's anti-fraud programme for review as it is a strategically important area. UN Women adopts a zero-tolerance policy towards fraud. Fraud is a reputational, operational and financial risk that can have impacts on an organization's ability to achieve its objectives.

Management is responsible for establishing and implementing effective anti-fraud governance, risk management and internal controls. 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 UN Women's existing anti-fraud programme, in particular:

- **Governance**: roles, responsibilities, capacity and resources, as well as instilling and enacting an anti-fraud culture, communication and tone-at-the-top, where zero tolerance to fraud is clearly understood and appreciated.
- **Adequacy of anti-fraud and corruption policies**: progress, achievements, gaps and duplications among existing policies and any areas for improvement.
- **Cost-effectiveness of preventative and detective controls**: process for identifying key fraud risks (e.g. programme partner risks) and controls to address those risks. This includes validating the risks identified by management and the related controls and evaluating the effectiveness of the fraud risk assessment process.

IAS reviewed five key anti-fraud areas **(**fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective actions, and fraud monitoring activities**)** using a maturity assessment model developed by the Association of Certified Fraud Examiners (ACFE). The maturity assessment model (see detailed definitions of each level in Section III) assessed each of the above elements on the following scale:

Level 1	Ad hoc
Level 2	Initial
Level 3	Repeatable
Level 4	Managed
Level 5	Leadership

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

Audit opinion and overall audit rating

IAS assessed the maturity level of the anti-fraud programme at UN Women as **Level 2 (Initial)** with some elements of **Level 3 (Repeatable)** identified, including: defined and standard policies and processes that are repeatable, and a fraud risk management process that is integrated with the enterprise risk management (ERM) programme. IAS recommends that UN Women advance its anti-fraud programme to **Level 4 (Managed),** which according to the Enterprise Anti-Fraud Maturity Assessment Model[1] means that (among other things): *fraud risk management activities across the organization are aligned with controls and performance indicators; performance and quality are defined and can be measured; information on fraud risks is aggregated and can be analysed and is easily available to management, including a process for notifying management in changes to fraud risk profiles is established and operating; and, full integration of the fraud risk principles into management processes has been achieved*.

IAS believes that the target maturity level is reasonable and feasible to implement within two to three-year period, subject to resource availability. Improvement in key

[1] Grant Thornton's Enterprise Anti-fraud Maturity Assessment Model©, presented within the ACFE's Anti-Fraud Playbook.

areas is subject to sufficient resources being made available or reallocated to enact the changes; strong senior management leadership; and tone at the top to articulate management's vision on integrity and anti-fraud culture. Investment in this area could help ensure maximum funds available for beneficiaries; prevent future financial loss, sustain donor interest and confidence; reduce time spent dealing with issues; and increase personnel's motivation. IAS recommends that management develops an action plan, accompanied with the resources required to implement it, noting the actions to be taken as part of existing workplans and responsibilities, as well as the actions which would require additional resources. This action plan with resource estimates should be presented to the Business Review Committee (BRC) for its consideration and recommendation for Executive Leadership Team decision.

To advance to the next level of maturity, UN Women should take the following actions:

- **Fraud risk governance**: UN Women has an Anti-Fraud Policy, but needs to clarify authority, responsibility and business process ownership for leading anti-fraud efforts in the organization, i.e. there was no plan to operationalize the Anti-Fraud Policy. UN Women needs to: (a) update fraud definitions and tolerance levels and make them consistent across various policies; and (b) improve tracking, compliance, and accountability for mandatory anti-fraud training. Regardless of which unit or function is assigned to lead/implement these recommendations sufficient resources need to be provided to finalize implementation and sustain the anti-fraud programme.
- **Integrity and anti-fraud culture:** In its 2020 review of ethics and integrity, IAS stressed *"the ethics and integrity were of concern to the Executive Leadership Team which made a serious effort to set the standard of behaviour across the Entity and to embed ethics and integrity into the fabric of UN Women's culture. This is to be recognized and applauded."* IAS recommended that senior management *"articulate its ethics and integrity strategy to demonstrate that UN Women will ensure its arrangements support and sustain the ED's aspirations for a well-developed ethics and integrity culture across UN Women."* IAS observed that this ethics and integrity culture still needs to be strengthened, including a dedicated integrity and anti-fraud vision, strategy and communications. The recommendations on culture in the ethics and integrity and anti-fraud reviews could be addressed concurrently, possibly integrating common elements to save on required resources.
- **Fraud risk assessment**: Fraud risk assessment processes have improved since they were introduced in 2018. This has been achieved with only one part-time staff member from the ERM function assigned to conduct these activities. The inherent risk is that efforts might be strictly focused on complying with minimum requirements rather than substantial actions and awareness against fraud and corruption. Improvements need to be focused on fully investing in an online risk management system (looking into different available off-the-shelf apps) in terms of recording, consolidating, and analysing the results for an integrated anti-fraud programme; engaging offices to identify and manage their specific fraud risks beyond standard/generic risks; and requiring specific fraud risk assessments for headquarters units and business process owners. UN Women needs to formalize risk reporting and escalation protocols for senior management decision-making.
- **Fraud control activities**: UN Women could consider how best to maximize the control automation in the incoming NextGenERP to capture and generate reports on potential red flags, exceptions, and deviations; utilize data analytics techniques to detect and prevent potential fraud as consolidated efforts for continuous monitoring; and, based on this, devise a fraud data analytics strategy. A detection and enforcement mechanism could also be developed to ensure the use of key controls such as the e-procurement system and background checks.
- **Fraud investigation and corrective action:** The current UN Women Legal Policy for Addressing Non-Compliance with UN Standards of Conduct does not give the authority to discharge responsibility for investigations to another office than UN Women's outsourced investigations provider, currently the UN Office of Internal Oversight Services (OIOS), and it does not foresee imposing disciplinary measures without an investigation. However, some matters reported may not warrant a full investigation because the evidence may be clear enough for management to take a management action, in principle, or a disciplinary action based on a short investigation. The matter may also not require serious disciplinary action and could be dealt with through reprimand, financial recovery, or other disciplinary measure. Investigation timelines have been long. IAS recommends that UN Women consider potential options for lower risk, lower exposure, or less grave issues that could be potentially investigated by independent, trained, and capacitated professionals

outside of the current set-up. However, UN Women's policy and procedures would need to be updated to accept and accommodate such an approach. Management also should provide sufficient resources to cover its end-to-end investigation processes.

- **Monitoring the effectiveness of the anti-fraud programme**: Monitoring of the effectiveness of the anti-fraud programme is largely not conducted. UN Women needs to develop a fraud monitoring programme that integrates the anti-fraud elements included in existing policies.

IAS made 12 recommendations to address the above areas for improvement. Five recommendations are ranked high priority and eight are medium priority.

The five high priority recommendations mean *"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."* These recommendations are presented below:

Recommendation 1 (High): The BRC in its role as Risk Management Committee to reassign responsibility from IEAS to an appropriate business process owner with the clear accountability and accompanied sufficient authority, capacity and resources to implement the overall Anti-Fraud Programme and coordinate its governance, fraud risk assessment, internal control system, and monitoring with the necessary support and engagement from other contributing business process owners along the three lines of defence model.

Recommendation 2 (High): The business process owner to revise the Anti-Fraud Policy in terms of roles and responsibilities, and its ownership in line with the three lines of defence model. In particular: a) Assign the key contributors to the policy, including senior management or specific key business process owners and IEAS (in its capacity as the designated office in supporting investigation-related activities, including the oversight and advisory role of the Advisory Committee on Oversight); b) Reassign responsibility for fraud monitoring across the three lines of defence in the Anti-Fraud Policy, ensuring consistency with related policies and appropriate legal instruments (such as the Partner Agreement); c) Establish a formal matrix of responsibility within the Anti-Fraud Policy for the various anti-fraud activities that refers to specific roles, functions, divisions and units in the organization; d) Request that policy owners take stock of key anti-fraud activities foreseen in their policies and, based on this exercise, align the activities with the Anti-Fraud Policy, either directly or through referral to those policies within their own fraud sections; and, e) Request that the PPG function include in the PPG Policy a requirement for key policies, when developed or reviewed, to specifically include controls to prevent, detect and correct -fraud with reference to the overarching Anti-Fraud Policy.

Recommendation 3 (High): The business process owner to coordinate with other key contributors (including HR, PSMU, Legal and IEAS) and develop an action plan with clear objectives, roles, resources and activities to operationalize the Anti-Fraud Policy, once it has been revised, to address the issues raised in this report. Implementation of the action plan should be reported to senior management and governing bodies.

Recommendation 10 (High): The UN Women Executive Office, in consultation with IEAS, Legal, HR and OIOS, to: a) Consider whether to continue with the current outsourced case intake and assessment measures, or to potentially establish internal triage protocols with clear criteria where formal grievances are reviewed and referred to the appropriate function (e.g., OIOS, IEAS, HR, PSMU, HQ/Regional, Country Office management, UN Ethics Office etc.) with due consideration to the nature, complexity, credibility and materiality of the complaint, and the need for any whistle-blower protection; b) Update the legal policy framework for UN Women that codifies its investigative, disciplinary and non-disciplinary (including referrals to national authorities) protocols for staff, other personnel and third parties (e.g. vendors, programme partners), as well as investigation outsourcing arrangement, addressing fact-finding/investigation roles to be potentially performed by independent UN Women parties and what will be outsourced; and, c) Update the investigations portion of the IEAS charter as relevant.

Recommendation 11 (High): The UN Women Executive Office, together with Chief, IAS, Legal and Director, IEAS to: a) Ensure that key performance indicators are devised and tracked that set expected investigation processing times and escalation in the event that cases take long to resolve; b) Ensure the Director, IEAS, who is involved in supporting the investigation function is appropriately resourced.

In addition, IAS made seven 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: align the definitions of fraud and corruption and highlight UN Women's zero tolerance policy; improve fraud and corruption training compliance; improve the culture of anti-fraud in the organization; strengthen fraud risk assessments; improve fraud risk ratings; develop protocols for fraud risk reporting; strengthen fraud detection and prevention; and define the nature, scope, frequency and measurement of anti-fraud monitoring.

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

Some recommendations in this report will be presented to the UN Women Business Review Committee for management to appoint a business process owner for certain anti-fraud activities. The action plan and timeframe for implementing recommendations will be updated after the decision is taken. Moreover, management involved in UN Women's anti-fraud activities including DMA, SPRED, and Legal Office reviewed and commented on the report, and provided action plans for some recommendations.

Lisa Sutton, Director
Independent Evaluation and Audit Services

ACRONYMS AND ABBREVIATIONS

ACFE	**Association of Certified Fraud Examiners**
BRC	**Business Review Committee**
CPI	**Corruption Perception Index**
DMA	**Division of Management and Administration**
ERM	**Enterprise Risk Management**
ERP	**Enterprise Resource Planning**
HR	**Human Resources**
IAS	**Internal Audit Service**
IEAS	**Independent Evaluation and Audit Services**
JIU	**Joint Inspection Unit**
KPI	**Key Performance Indicator**
OIOS	**United Nations Office of Internal Oversight Services**
PPG	**Policy, Procedure and Guidance**
PSMU	**Programme Support Management Unit**
SPRED	**Strategy, Planning, Resources and Effectiveness Division**

I. INTRODUCTION

An anti-fraud programme in general includes the set of policies, procedures, guidance, practices and culture, and efforts by an organization's personnel, that address fraud, including fraud prevention, detection and correction. UN Women's Anti-Fraud Policy notes that *"UN Women, as a potential victim of fraud, is exposed to various risks which may include: financial risks, which can be measured in monetary terms; operational risks, which cause deficiencies in the implementation and delivery of programmes; and reputational risks, which harm the prestige and respect of the Organization."* Therefore, in its 2021 risk-based audit plan, IAS included an audit of UN Women's anti-fraud programme because it is a strategically important area.

This is the first internal audit of UN Women's anti-fraud programme. In 2016, the Joint Inspection Unit (JIU) conducted a review of "Fraud Prevention, Detection and Response in United Nations System Organizations". Key recommendations included the need for UN Women to: adopt common definitions of fraudulent and other practices; develop an anti-fraud policy; designate a senior person/entity to be custodian of the anti-fraud policy; establish an anti-fraud training and fraud awareness strategy; conduct a corporate fraud risk assessment; develop anti-fraud strategies; ensure anti-fraud controls form part of the internal control framework; introduce a statement of internal controls; update legal instruments for engaging third parties with anti-fraud clauses; include fraud prevention and detection capabilities in automation systems' functionalities; update whistle-blower policies; establish a central intake mechanism for all fraud allegations; ensure the investigative function has key performance indicators (KPIs) for conduct and completion of investigations; strengthen protocols for referrals of fraud cases; present an annual report to governing bodies on anti-fraud activities; and governing bodies should have a standing agenda item on anti-fraud issues.

Of the 16 JIU recommendations, UN Women did not accept 1 recommendation (on strengthening protocols for referrals of fraud cases) and assessed 14 of the remaining 15 recommendations as implemented. One recommendation (#8) remained in progress at the time of audit, linked to introducing or updating statements of internal controls.

II. BACKGROUND

The UN system-wide common definition of fraud is included in UN Women's Anti-Fraud Policy effective 20 June 2018:

"Any act or omission whereby an individual or entity knowingly misrepresents or conceals a material fact (a) in order to obtain an undue benefit or advantage for himself, herself, itself, or a third party, and/or (b) in such a way as to cause an individual or entity to act, or fail to act, to his, her or its detriment" (High-Level Committee on Management, 33rd Session, March 2017).

UN Women's anti-fraud programme

UN Women's anti-fraud programme includes several elements such as:

- **Governance**: An Anti-Fraud Policy, first issued in April 2017 and updated, effective as of June 2018. The policy also refers to other key policies, described below.

- **Risk assessment**: Annual fraud risk assessments for headquarters and field offices were first introduced in 2018, led by the enterprise risk management (ERM) function. These assessments are governed by the Risk Management Policy and Procedure and supported by the Fraud Risk Assessment Guidance.

- **Internal controls**: Individual processes are guided by policies, procedures and guidelines (see below), e.g., Special Service Agreements (SSA) for recruitment and management of individual consultants; procurement including ethics, fraud, corruption and bribery; programme management policies including requirements to build partner capacity in anti-fraud measures, etc. Key preventive and detective fraud controls include contract review committees, delegation of authority and approval thresholds, and segregation of duties requirements across various organizational functions.

- **Investigation**: UN Women engages an external investigation service provider, currently the United Nations Office of Internal Oversight Services (OIOS), based on a Memorandum of Understanding (MoU). The Director, IEAS is the designated official responsible for coordinating investigation-related matters. UN Women's Legal Policy for Addressing Non-compliance with UN Standards of Conduct defines the investigation process, roles and responsibilities. An internal standard operating procedure advises how to handle OIOS referrals to UN Women management (i.e., allegations where

investigations are not opened, but that are referred to management for potential action as deemed necessary).

- **Monitoring**: Monitoring activities are limited; however, the Executive Board reviews IAS' annual report on internal audit and investigation activities (drawing on information provided and work performed by OIOS), as well as the Executive Director's annual report on disciplinary measures and other actions taken as a result of fraud and other investigations.

Key overarching policies and procedures covering fraud

Several corporate policies and procedures either address or are related to fraud, including the Anti-Fraud Policy, the Internal Control Framework, the Delegation of Authority Framework, the Legal Policy for Addressing Non-Compliance with UN Standards of Conduct, the Protection Against Retaliation Policy, the OIOS Referrals Decision Grid, the Risk Management Policy and Procedure, the Fraud Risk Assessment Guidance and the Charters of the Independent Evaluation and Audit Services and the Internal Audit Service. The Due Diligence Policy, which assesses the risks and benefits of potential alliances or partnerships, has a primary purpose of protecting UN Women from operational and reputational risks.

Anti-fraud roles and responsibilities

Responsibility for anti-fraud activities falls on a range of parties within headquarters and the field. The UN Women Anti-Fraud Policy (issued in 2017, updated in 2018 and due for review in 2022) is owned by the Division of Management and Administration (DMA) and sets the overall parameters and tone for anti-fraud in the organization. DMA is responsible for maintaining the policy. However, the policy also notes that *"IEAS shall act as the corporate manager who is the custodian of this Policy and who is responsible for the implementation, monitoring, and periodic review of this Policy."* The policy was issued before IEAS was fully established and staffed.

Anti-fraud provisions and tools are embedded in other policies and implemented by several units and divisions as follows:

- The Advisory Committee on Oversight's terms of reference note that the committee will "*review and advise on the fraud and corruption prevention policies and activities, the code of ethics and whistle blower policy."*
- The Business Review Committee (BRC) serves as the Risk Management Committee to provide advisory support and oversee the monitoring and evaluation of risk management at UN Women, including fraud risk management.
- The Risk Management Committee leads implementation and management of fraud prevention and detection controls designed to manage potential risks that may expose the organization to fraud. These activities are in accordance with the Anti-Fraud Policy and, along with the Risk Management Procedure, include mechanisms and measures to assess and manage fraud risk.
- The Policy, Programme and Intergovernmental Division (PPID) is responsible for programme partner management including fraud awareness training for field offices and programme partners.
- The Procurement team is responsible for managing the Contract and Procurement Management Policy and e-procurement system, which include fraud prevention and detection controls.
- The Financial Management Section manages financial controls, the partner cash advance process, asset write-off and other areas.
- The Human Resources Division manages anti-fraud controls in recruitment, and is a focal point for ethics and liaising with the UN Ethics Office. The division also has anti-fraud responsibilities in terms of engagement of individual contractors, outside activities and conflicts of interest.
- The ERM function is responsible for administering fraud risk assessments and categorizing and tracking these assessments within the organization, while also championing the provision of training in this area.
- The Legal Office advises on fraud risks and emerging issues.
- Intake and assessment of fraud allegations, as well as fraud investigation are performed by OIOS.
- At individual engagement level, IAS has a responsibility to consider fraud red flags and the adequacy of internal controls during activity-level risk assessments. IAS designs audit procedures to test these controls and advises management on fraud risks.

- The Director, IEAS has the authority to assist OIOS investigation activities, including: tracking OIOS case data and preparing statistics (e.g. Advisory Committee on Oversight and the IAS annual report); coordinating related information requests; providing OIOS with requested data and records; following up on OIOS investigation reports and referrals to management; preparing and following up on lessons learned with management; performing proactive and reactive integrity (or red flag) reviews where applicable; and promoting fraud awareness.

- All UN Women personnel are required to complete a two-hour online mandatory training course on anti-fraud policies when they join UN Women.

Fraud risk assessments

Fraud risk assessments were introduced in 2018 and at the time of this audit review were coordinated by the Strategy, Planning, Resources and Effectiveness Division (SPRED) after the ERM function was moved from DMA. Risk assessments have to be completed or updated at least yearly for each field office and headquarters unit. The most recent round of fraud risk assessments was administered by field offices in Q1, 2021. At the time of the audit, the latest round of headquarters fraud risk assessments had not yet been completed and the corporate fraud risk assessment had not yet been consolidated.

SPRED is endeavouring to devise a risk profile for each field office with ten criteria, of which fraud risk assessment results is one. This should help Regional Offices and headquarters management assess the level of support needed by each office. As part of this exercise, offices are required to link key fraud risks with existing internal controls to assess the impact and likelihood of fraud risks. SPRED provides training to field offices on how to complete and quality assure fraud risk assessments.

Investigations

OIOS provides investigation services to UN Women. The Investigations Division of OIOS assesses and, as needed, investigates allegations of fraud, corruption or other wrongdoing by UN Women personnel or by third parties to the detriment of UN Women. OIOS establishes the facts that will allow UN Women senior management to take appropriate action, including initiating disciplinary proceedings or other sanctions. OIOS has established a reporting facility, i.e., a confidential mechanism for individuals wishing to report fraud, mismanagement and other types of misconduct.

III. AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

The audit objectives were to assess the effectiveness of the existing anti-fraud programme, in particular:

- **Governance**: roles, responsibilities, capacity and resources, as well as instilling and enacting an anti-fraud culture, communications and tone-at-the-top, where zero tolerance to fraud is clearly understood and appreciated.

- **Adequacy of anti-fraud and corruption policies**: progress, achievements, gaps and duplications among existing policies and any areas for improvement (e.g., a policy which has not been fully operationalized into practical applications).

- **Cost-effectiveness of preventative, detective and corrective controls**: process for identifying key fraud risks and controls to effectively address those risks. This includes validating the risks and controls identified by management and evaluating the effectiveness of the fraud risk assessment process.

This was achieved through reviewing the following five key anti-fraud areas, as delineated by the Association of Certified Fraud Examiners (ACFE) as shown in Table 1.

Table 1: ACFE five key fraud areas

#	Section	Description
A	Fraud risk governance	• Governance arrangements with respect to anti-fraud programmes throughout the organization, including clarity around accountability, roles and responsibilities, and capacity of key actors • Culture in the organization with respect to fraud and corruption
B	Fraud risk assessment	• Effectiveness of risk assessments of fraud risks performed by managers and business process owners
C	Fraud policies and control activities	• Adequacy of anti-fraud policy designed to mitigate fraud and corruption risks – mapping existing policies to best practices and identifying the gaps to be addressed in policies • Effectiveness and efficiency of key internal controls for preventing and detecting fraud, including training and awareness, monitoring and early warning and detection • Use of systems to facilitate anti-fraud efforts such as reporting on exceptions, red flags and other tools of continuous monitoring
D	Fraud investigation and corrective action	• Process for investigating suspected fraud • Process for disciplining and sanctioning of personnel and vendors • Effectiveness of fraud reporting and follow-up mechanisms • Lessons learned and revision of policies to reflect emerging risks
E	Fraud monitoring activities	• Monitoring of compliance with anti-fraud policies and procedures • Performance measures and reporting for anti-fraud function (Key Performance Indicators [KPIs] and periodic assessments of anti-fraud programme)

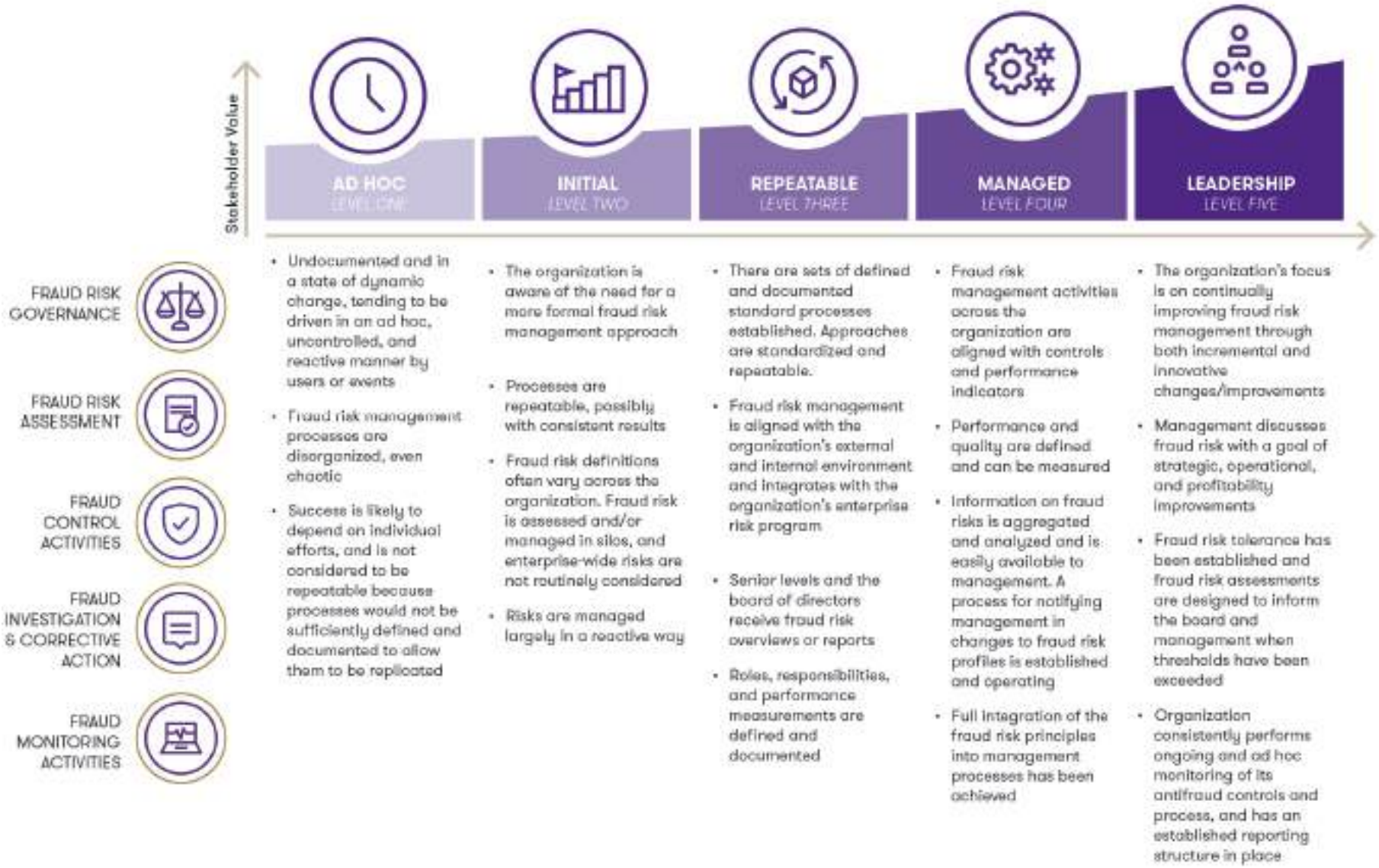
Scope disclosures

The anti-fraud programme audit objectives and maturity assessment model include the need to review fraud investigation as part of section D of the model's objectives. IAS may not be able to fully assess the effectiveness of investigation arrangements at UN Women or the performance of OIOS. However, the audit still aimed to review key aspects related to fraud investigations and recommend improvements required in the management of the service provision.

Methodology

The audit made use of a maturity assessment model to assess UN Women's anti-fraud performance. The Enterprise Anti-Fraud Maturity Assessment Model was developed by Grant Thornton and was endorsed by the Association of Certified Fraud Examiners (ACFE). The maturity assessment model is outlined in Figure 1 and the audit assessed UN Women's performance in each of the five objective areas. The audit was supported by a senior anti-fraud and investigations expert from OIOS.

Figure 1: Anti-Fraud Programme Maturity Model (Source: Association of Certified Fraud Examiners)



IV. AUDIT RESULTS

A. OVERALL ASSESSMENT

IAS assessed the maturity level of the anti-fraud programme at UN Women as **Level 2 (Initial)** with some elements of **Level 3 (Repeatable)** identified, including: defined and standard policies and processes that are repeatable, and a fraud risk management process that is integrated with the ERM programme. IAS recommends that UN Women advance its anti-fraud programme to **Level 4 (Managed),** which according to the Enterprise Anti-Fraud Maturity Assessment Model means that (among other things): *fraud risk management activities across the organization are aligned with controls and performance indicators; performance and quality are defined and can be measured; information on fraud risks is aggregated and can be analysed and is easily available to management, including a process for notifying management in changes to fraud risk profiles is established and operating; and, full integration of the fraud risk principles into management processes has been achieved.*

The sections below present the findings of the maturity assessment and proposals for management consideration, including:

- As a priority and prerequisite for other policy improvements, sufficiently addressing the anti-fraud risk management and related controls and enhancing the anti-fraud policy framework, consisting not only of the Anti-Fraud Policy but also related policies accompanying the internal control framework, ensuring consistency and comprehensiveness of approach.
- Devising action plan for consolidating and institutionalizing the efforts already taken by the organization to advance its anti-fraud programme, as well as methods and tools for anti-fraud detection and prevention and an overall anti-fraud programme effectiveness monitoring.

Table 2 briefly summarizes the current assessed maturity level and target level for long-term maturity proposed by IAS, based on the maturity model presented on page 5. The level definitions are proposed by the Association of Certified Fraud Examiners. The target levels proposed by IAS are being reasonable and feasible to implement within a two to three-year period. Improvement in all attributes is subject to sufficient resources being made available or reallocated to enact the changes; strong senior management leadership; and tone at the top to articulate management's vision on integrity and anti-fraud culture.

Table 2: Comparison of current maturity level and target level maturity for anti-fraud programme process improvement

Anti-fraud programme attribute	Current level	Target level
1. Fraud risk governance	**Level 2: Initial**	**Level 4: Managed**
2. Fraud risk assessment	**Level 2: Initial**	**Level 4: Managed**
3. Fraud control activities	**Level 2: Initial**	**Level 4: Managed**
4. Fraud investigation and corrective action	**Level 3: Repeatable**	**Level 4: Managed**
5. Fraud monitoring activities	**Level 1: Ad hoc**	**Level 4: Managed**

B. FRAUD RISK GOVERNANCE

Issue 1: Roles and responsibilities

"The Fraud Risk Management roles and responsibilities of all personnel should be formally documented. This includes the board of directors, audit committee, senior management, business-enabling functions, risk and control personnel, legal and compliance personnel, and all other employees, as well as other parties interacting with your organization, such as contractors and customers." (ACFE Anti-Fraud Playbook)

Roles and responsibilities

The Anti-Fraud Policy was approved by the Director, DMA on 20 June 2018, before IEAS was fully established and staffed. The Anti-Fraud Policy states that the *"Director, IEAS shall act as the corporate manager who is the custodian of this Policy and who is responsible for the implementation, monitoring, and periodic review of this Policy. In carrying out this role, the Director, IEAS will among other things: a) serve as the repository of knowledge on fraud risks and controls; and b) manage the fraud risk assessment process and co-ordinate anti-fraud activities across the Organization."* This is not an appropriate set of roles and responsibilities for the Director, IEAS to have. While the Director, IEAS has a clear role in anti-fraud activities in the organization, the

Director cannot be responsible for implementing management activities. Section 20 of the Charter of the Internal Audit Service (IAS) states that the Director of IEAS and IAS staff are not authorized to *"perform any operational duties for UN-Women or its affiliates"* or *"have direct operational responsibility or authority over any of the activities reviewed".* IAS benchmarked this provision with other UN system organizations, and none included IEAS as the anti-fraud policy custodian.

Other than the Director, IEAS, the Anti-Fraud Policy lists the responsibilities of general categories of personnel including personnel, managers, vendors and programme partners and responsible parties (*the names of which are out of date with respect to programme management policies*). The policy has a reference to the three line of defence model; however, it does not define specific responsibilities for management oversight and monitoring (or other anti-fraud activities) to "business-enabling functions" or so-called business process owner for Anti-Fraud Policy and Programme. The Anti-Fraud Policy does not adequately state who is responsible for ensuring the implementation, monitoring of its effectiveness and adjustment of the policy. While implementation of the Anti-Fraud Policy is the responsibility of all first and second line of defence managers, the policy should have one business process owner to coordinate its implementation. In practice, Anti-Fraud Policy activities are mainly implemented by the Risk Manager (reporting to the Director, SPRED) who coordinates the risk assessment process for operational and fraud risks and trains focal points in the field.

The policy does not establish the responsibility of business process owners (e.g., for procurement, finance, HR, etc.) to identify risks and monitor red flags in their respective policies. Neither does the policy address the roles of the Executive Board, Advisory Committee on Oversight (although the committee's terms of reference do address anti-fraud) or senior management.

IEAS' fraud monitoring role should therefore be revised in the Anti-Fraud Policy. The policy should also clearly state the fraud monitoring roles within the first and second lines of defence. The policy should establish a matrix of responsibility among key contributing business process owners, assigning appropriate responsibility for appropriate areas (e.g., the Director, HR is responsible for HR-related anti-fraud activities).

The Anti-Fraud Policy has not been accompanied by an anti-fraud procedure or action plan, which usually serve to operationalize the high-level and principle-based policy. Such a procedure or action plan would cover key elements of policy implementation such as anti-fraud programme monitoring arrangements to ensure that the programme is effective, i.e., clarifies KPIs for anti-fraud programme effectiveness; how they are monitored and reported; and by whom. The policy should also be clearly linked to the fraud risk assessment process and internal control system (see Issue 8 on fraud detection and prevention). Responsibility should also be assigned and described for key anti-fraud awareness and communication efforts and related activities including the nature, timing, frequency and extent of anti-fraud communications from executive and senior management.

The Anti-Fraud Policy does not address fraud risk. Fraud risks are covered by the Risk Management Policy, but the Anti-Fraud Policy does not refer to it, nor is the content linked together. For example, the Anti-Fraud Policy does not discuss how fraud risks are to be monitored, or how fraud risk assessments are relevant to anti-fraud programme, which represent an important element of the integrated corporate anti-fraud programme and its implementation cycle (see the example in Figure 2 from the ACFE). The Risk Management Policy also does not address this, merely including fraud risks as another type of risk to be managed.

Figure 2: ACFE Fraud risk management cycle (source: ACFE)

Lastly, the Anti-Fraud Policy does not always address fraud and corruption roles and responsibilities in key operational and programmatic areas, e.g., duty travel, assets, cybersecurity, Special Service Agreement Policy, Service Contract Policy and the Recruitment Selection Guidance, among others. While there are links to some related policies (such as procurement) at the end of the Anti-Fraud Policy, others (such as those listed above) are not included, and their own policies do not explicitly address fraud.

The following concerns were raised in discussion with SPRED and DMA:

- DMA previously led anti-fraud as JIU recommendations were assigned to DMA. In particular, DMA led policy development and briefed the Executive Board on implementation progress.
- After headquarters restructuring, several units involved in the anti-fraud programme moved from DMA. The ERM function moved to SPRED, together with the audit coordination unit, and the Legal Office was restructured into an independent office. Moreover, the HR Division as a business process owner for HR fraud risk management was also restructured into an independent office. At the time of audit, DMA did not have dedicated resources to coordinate the anti-fraud programme.
- SPRED's ERM function has been advancing the fraud risk assessment exercise and training. However, the risk manager has two roles – ERM and PPG Framework management– both requiring enhanced capacity as identified in previous internal audit engagements. While a coordination role for the Anti-Fraud Programme would be a natural extension of ERM and PPG, the ERM function would need at least temporary corporate investment to finalize ongoing efforts which could be then be embedded into its risk management activities.

In some UN agencies, the anti-fraud function resides within various units including bureau for management services, department of financial and administrative management, department of management or the ERM function.

Recommendation 1 (High):

BRC in its role as Risk Management Committee to reassign responsibility from IEAS to an appropriate business process owner with the clear accountability and accompanied sufficient authority, capacity, and resources to implement the overall Anti-Fraud Programme and coordinate its governance, fraud risk assessment, internal control system, and monitoring with the necessary support and engagement from other contributing business process owners along the three lines of defence model.

Recommendation 2 (High):

The business process owner to revise the Anti-Fraud Policy in terms of roles and responsibilities, and its ownership in line with the three lines of defence model. In particular:

a) Assign the key contributors to the policy, including senior management or specific key business process owners, IEAS (in its capacity as the designated office in supporting investigation-related activities), and the oversight and advisory role of the Advisory Committee on Oversight.

b) Reassign responsibility for fraud risk monitoring across the three lines of defence in the Anti-Fraud Policy, ensuring consistency with related policies and appropriate legal instruments.

c) Establish a formal matrix of responsibility within the Anti-Fraud Policy for the various anti-fraud activities that refers to specific roles, functions, units and divisions.

d) Request that the PPG function include in the PPG Framework Policy a requirement for key policies, when developed or reviewed, to specifically include controls to prevent, detect and correct fraud with reference to the overarching Anti-Fraud Policy.

e) Request that policy owners take stock of key anti-fraud activities foreseen in their policies and, based on this exercise, align the activities with the Anti-Fraud Policy, either directly or through referral to those policies within their own fraud sections.

The 2016 JIU review of "Fraud Prevention, Detection and Response in United Nations System Organizations" found that *"even in organizations that have a corporate stand-alone anti-fraud policy, a clear definition of roles, responsibilities and accountabilities is*

missing and there is lack of clear guidance on how to operationalize the policy." This is also true of UN Women. While the Entity has an Anti-Fraud Policy, no plan or mechanism is in place to operationalize it. The Anti-Fraud Policy is mainly enacted through conducting individual office fraud risk assessments (although this process is not addressed in the Anti-Fraud Policy). These assessments are not consolidated, validated and then acted upon by senior decision makers to enhance corporate efforts in fighting fraud and corruption, enhance its internal control system and to focus on processes with more frequent risks.

Recommendation 3 (High):

The business process owner to coordinate with other key contributors (including HR, PSMU, Legal and IEAS) and develop an action plan with clear objectives, roles, resources and activities to operationalize the Anti-Fraud Policy, once it has been revised, to address the issues raised in this report. Moreover, to include in the Anti-Fraud Programme action plan an analysis performed by respective business process owners of risks, controls and key gaps. Implementation of the action plan should be reported to senior management and governing bodies.

Also, addressing Issue 4 below, the business process owner to include a set of actions to improve UN Women's anti-fraud culture, awareness, training and communications in the anti-fraud programme action plan.

Issue 2: Aligning definitions of fraud and misconduct

"Our fraud risk management policy and fraud training define fraud, identify both internal and external potential perpetrators of fraud, provide hypothetical organization-based examples of fraud, and define the roles and responsibilities of those charged with oversight of fraud control." "Our fraud risk management policy articulates our risk tolerance considerations and the expectation that suspected fraud will be reported immediately." (ACFE Fraud Risk Governance Scorecard)

The definition of fraud in UN Women's Anti-Fraud Policy is not fully consistent with fraud definitions in other key policies. The Anti-Fraud Policy states that "the UN system wide common definition of fraud is *'any act or omission whereby an individual or entity knowingly misrepresents or conceals a material fact (a) in order to obtain an undue benefit or advantage for himself, herself, itself, or a third party, and/or (b) in such a way as to cause an individual or entity to act, or fail to act, to his, her or its detriment'",* which is from the High-Level Committee on Management (HLCM), 33rd Session, March 2017. The policy does not specifically address related terms such as corruption or collusion and the extent to which they are addressed (or not addressed) by the policy.

The definition of fraud was not consistent across various policies, including the Contract and Procurement Management Policy (the only policy that currently defines fraud and corruption), the Legal Policy for Addressing Non-Compliance with UN Standards of Conduct (which is predominantly meant to address cases of misconduct including fraud among others), the Risk Management Policy and Procedure and Fraud Risk Assessment Guidance (which do not include a fraud definition, but mention fraud risks). Some policies have an expanded definition which includes corruption, collusion and coercion. The Memorandum of Understanding signed by UN Women with the Multi-Partner Trust Fund Administrative Agent has an expanded definition[2], which IAS suggests is also adopted by UN Women. Similar to the Procurement Policy, the Memorandum of Understanding for the Spotlight Initiative also defines corrupt, collusive, coercive, unethical and obstructive. Benchmarking against other UN entities, UNICEF's fraud policy (2013) defines fraud, corruption, collusion, coercion and obstruction; the UNFPA fraud policy (2018) also does so and includes a definition of unethical practice; the UNOPS policy (2018) defines fraud and corruption and provides relevant examples which may aid the reader's understanding; and the FAO fraud policy (2016) also defines these terms and includes *"improper use of the Organization's resources",* and includes examples of what the definitions may look like in practice.

Moreover, the Anti-Fraud Policy and Risk Management Policy and Procedure do not state UN Women's zero tolerance principle to fraud and corruption. Moreover, the fraud risk tolerance level is not clearly defined to:

[2] The language is from the Standard Memorandum of Understanding for MDTFs and JP, that has been agreed upon by the members of the United Nations Sustainable Development Group (UNSDG), 2019, which refers to "fraudulent practices" as *"any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, an individual or entity to obtain a financial or other benefit, or to avoid an obligation"*

- inform all other activities, including the way in which the Entity pursues disciplinary action or corrects for fraud;
- help management make value-driven and cost-effective investment decisions on the appropriate level of fraud controls;
- be clearly linked and incorporated with the Risk Management Policy, procedure and communications including fraud risk management; and
- inform investigative and corrective action, and the extent of fraud detection monitoring activities to be undertaken.

Recommendation 4 (Medium):

The business process owner and Director, SPRED to:

a) Include UN Women's zero tolerance principle, risk tolerance and appetite to fraud and corruption in the Anti-Fraud Policy and Risk Management Policy and Procedure.

b) Establish a mechanism to ensure other business process owners align the definitions of fraud throughout their relevant PPG.

c) Consider expanding definitions in the Anti-Fraud Policy to include topics such as corruption and other unethical practices.

Issue 3: Fraud and corruption training and awareness

"Assess the effectiveness of the enterprise-wide mandatory fraud training against the stated learning objectives using an established methodology, such as pre- and post-training surveys to compare the level of understanding of the skills and concepts before and after the seminar. Adjust the training approach and materials based on the results. Adapt the enterprise-wide mandatory fraud training periodically to address new fraud schemes, fraud risks, regulations, policies, etc." (ACFE Anti-Fraud Playbook)

Anti-Fraud Policy training requirements

One of UN Women's seven mandatory training courses covers fraud and corruption awareness and prevention. The two-hour online training course was developed for use by UNDP, UNCDF, UNFPA and UN Women and is hosted on UNICEF's Agora online training platform. The course content includes an overview of fraud and corruption, awareness and prevention methods, and reporting fraud and corruption. The course content is presented and discussed in an accessible manner for a wide audience. The training content appeared reasonable to provide all personnel with an awareness of fraud and corruption as well as their responsibilities for prevention and reporting.

UN Women, together with UNFPA and UNHCR, also developed a fraud awareness course for programme partners which is strongly recommended for partners and personnel working in programme and project management. In addition, as part of fraud risk management training, webinars were conducted with 151 personnel over three separate sessions. A stand-alone module on personnel's obligations was also included (covering standards of conduct, ethics and integrity, conflict of interest, etc.).

The HR Division's intranet site states that the mandatory fraud and corruption training should be completed by all new hires within the first six months of their arrival. There are no exceptions, for example based on the duration of a person's contract. The Anti-Fraud Policy does not refer to this training, but does refer to the also mandatory ethics and integrity training course and states that it must be completed *"within 90 days of arrival at UN Women".* These messages are inconsistent, and a three-to-six-month time frame may be too long. There is no guidance on when to retrain or update personnel knowledge nor there are tools to measure effectiveness of the training programme.

As stated by the ACFE, best practice is that organizations require annual anti-fraud training, as awareness and training are recognized as the most effective anti-fraud activities. In addition, surveys could be used to assess training effectiveness.

IAS' report on Ethics and Integrity Benchmarking stated that "*More needed to be done to ensure that the ethics and integrity refresher training was completed by all staff. There were no regular reminders or certification on ethics and integrity controls for individual managers. Good practice is for all staff to undergo annual ethics and integrity refresher courses and to mandate that personnel being promoted to supervisory roles or reassigned between headquarters and the field undergo enhanced ethics and integrity training (e.g., Leadership Dialogue)*." The report recommended that all staff undergo refresher training on an annual basis. As this topic is closely interlinked with anti-fraud programme, a similar approach should be taken for fraud and corruption awareness and prevention training programmes.

Compliance rate for anti-fraud mandatory training

As the anti-fraud training course is mandatory (which signifies its high importance) at any given time the number of personnel who have not completed the training should be approaching zero. The UN Women Strategic Plan 2018–2021 has a target of 85 per cent of offices to have completed training on anti-fraud and accountability. However, actual levels of completion are lower. As of 24 June 2021, 2,939 personnel[3] have completed the anti-fraud training (since its inception in 2018). Of these 2,939 personnel, 225 (8 per cent) took longer than 90 days to complete the training and 118 (4 per cent) took longer than six months to complete it, including four P5s, three P4s, five P3s and four National Officers at Level C (NOC). Further analysis found that 1,294 (38 per cent) of the 3,391 personnel employed by UN Women on 5 May 2021 had not completed the anti-fraud training. This included 175 personnel at P3 level or above (or 36 per cent of a total 488).

UN Women has a dashboard for monitoring mandatory training completion; however, at the time of the audit, the system was not working and not showing the data. It is possible that some personnel had completed the training when they were employed with another organization. There is a pending request to improve the training dashboard and to automate the updates, which has been on hold due to other urgent projects.

The performance management process asks staff to certify whether they have completed all mandatory training. As part of the performance management process, supervisors must ensure and verify that their teams have completed all mandatory training (including the anti-fraud training). However, the above analysis shows that, despite this, compliance remains an issue. Supervisors should be held accountable for the inaccurate disclosures they make in their performance management documents.

Need for more training

During its field audits, IAS has learned about potential wrongdoing instances which were dealt with directly by management without reporting to OIOS. This internal process was often not documented in organized or discrete manner. The personnel involved might have not had adequate knowledge, skills and authority on how to deal with the allegation(s), potentially compromising due process, confidentiality and the investigation process itself. Based on the recently piloted IAS surveys on ethics and working environment as part of country office audits, IAS has started receiving feedback that not all UN Women personnel know about their responsibility to report knowledge or suspicion of wrongdoing, or, that they know about their responsibility but do not know how to report or are not comfortable doing so. Therefore, there is a risk that some issues related to potential wrongdoing are not recorded and addressed properly.

Managers are responsible to prevent and detect the fraud, or, when an investigation is warranted, to ensure it is handled appropriately. Currently, UN Women does not have any fraud training aimed specifically at managers. Some organizations have induction training programmes for management, with annual or periodic updates, to train managers on how to receive reports of fraud and how to handle them.

Recommendation 5 (Medium):

The business process owner to:

a) Follow up on the pending request to improve the system for tracking the completion of mandatory training, and develop a mechanism to hold managers accountable for not ensuring all personnel complete the training. Institute accountability measures for non-completion of mandatory training, especially for senior personnel and those with budget management responsibilities.

b) Revise and align the mandatory training completion deadlines, ideally making them mandatory within the first 30 days

c) Develop annual refresher training.

d) Conduct periodic user surveys to assess the effectiveness of training materials.

e) Develop fraud reporting and fraud case handling training for managers to be delivered as part of manager induction and including periodic refreshers.

[3] As at June 2021, UN Women employed 3,470 personnel.

Issue 4: Strengthening anti-fraud culture

"When a person understands and appreciates that they have a responsibility to their organization, that they are accountable to its mission, and that they have the authority to effect positive change in that organization, a culture intolerant of improper or inappropriate conduct, such as fraud, is more likely to persist. The foundation of this concept is awareness. Promoting awareness among your employees about both the threat of fraud and their capacity to combat it is essential for creating an anti-fraud culture and can be a vital tool in fighting fraud in your organization." (ACFE Anti-Fraud Playbook)

Several observations support the conclusion that anti-fraud culture at UN Women could be strengthened.

First, the senior management forums did not periodically discuss or contribute to fraud awareness. The audit also observed low levels of communications on anti-fraud policies and initiatives. Of a total of 4,052 written media items on UN Women's external website, only three mentioned fraud and none mentioned anti-fraud efforts, while 38 items mentioned corruption, 27 of which are published before 2018. Of 110 emails from executive management addressed to the organization at large from 2018 to June 2021, only five made mention of fraud, including three emails on the annual report on disciplinary measures; one on the establishment of IEAS in 2018; and another on the launch of the fraud and corruption prevention training course in 2018. Fraud or anti-fraud was not mentioned in agendas from 21 UN Women global town hall meetings from 8 May 2018 to June 2021.

The annual reports on disciplinary measures and other actions (covering all types of misconduct) from 2013 to 2020 referred to a total of 11 cases involving staff; 20 cases involving consultants and contractors; 3 cases involving vendors; and 1 case involving a partner. No cases of fraud were listed for 2019 or 2020 (four in 2018 and ten from 2013–2017).

IAS has earlier reported a significant deficit in the number of personnel who have completed mandatory fraud and corruption awareness and prevention training, including 175 personnel at P3 level or above (see Issue 3). Senior personnel set an example for other personnel in what they do and do not do. IAS' field office audits often found that anti-fraud was not a regular topic of discussion in key meetings.

IAS raised a recommendation in its Ethics and Integrity Benchmarking Review (2020) that senior management needs to articulate its ethics and integrity strategy to ensure a well-developed ethics and integrity culture across the organization. As at the time of this report, the recommendations have not been addressed.

This issue has been addressed as part of Recommendation 3 above. As a part of the Anti-Fraud action plan, the importance of organizational culture, awareness, training and communications, should be addressed, including a strategy for improving it, and how and when to communicate anti-fraud topics.

C. FRAUD RISK ASSESSMENTS

Issue 5: Strengthening fraud risk assessments

"*A Fraud Risk Map is a resource that outlines identified potential fraud schemes and other related information for each scheme, such as actor and fraud risk entry point, for various areas across your organization and is a resource you will be able to employ across your fraud risk management activities.*" (ACFE Anti-Fraud Playbook)

UN Women revised its risk management framework in 2020, including updates to its Risk Management Policy and Procedure, and the fraud risk management process. Management introduced new and more detailed guidance on how to conduct enterprise risk and fraud risk assessments. The methodology for fraud risks assessments was essentially the same between 2020 and 2021, with a few updates. The 2020 fraud risk assessment included nine standardized risks with pre-set risk identification information; while the 2021 fraud risk assessment included 19 standardized risks. In both years, offices were required to complete the control assessment, residual risk analysis, risk treatment and risk monitoring and review sections. The significant expansion in the number of standardized risks included in the fraud risk assessment may represent improvement in the assessment's sophistication and level of detail. However, the lack of flexibility for offices to add their own risks based on their unique context and to tailor risk descriptions to that context may prevent offices from effectively addressing all key fraud risks and designing meaningful mitigating actions to address them, e.g., risks arising from cash for work initiatives, blockchain work, remote managing of beneficiaries, etc.

UN Women's OneApp system includes a module called the Risk Management System;

however, it is merely a repository. In its current form, the system cannot manage the entire fraud risk assessment process. Given the system's limitations, other tools are used such as the standardized fraud risk assessment that resides outside the system. In the past, the aim of the Risk Management System was to house all risks identified within the organization at the field office and headquarters unit level, including fraud risks. In practice, the system is mainly used to house non-fraud-related risks. The latest fraud risk assessment process (used in 2020 and 2021) for field offices was a manual process in which offices completed a template, signed it and then uploaded it to a SharePoint drop-box. In 2020, 51 individual field office fraud risk assessments were uploaded to the SharePoint. In 2021, 75 individual fraud risk assessments were uploaded.

Fraud risk assessments for headquarters units were not completed for 2020 or 2021, due to various factors such as competing priorities and limited resources available to coordinate the assessments. Business process owners have not conducted risk assessments to confirm that the risk library is complete and includes key fraud risks. In other benchmarked organizations, this process was used as a stocktaking exercise or baseline for the fraud risk assessments.

With missing fraud risk assessments from headquarters units and business process owners, the corporate risk assessment and fraud mitigation strategies cannot be completed effectively. This is an indication that the JIU recommendations related to corporate risk assessment and anti-fraud strategies have not yet been fully implemented. Moreover, manual processes limit the ability of management to analyse cross-functional risks holistically; assess risk management actions on common gaps; or scan for risks not identified at all. For example, recurring fraud risks in procurement, travel or consultant recruitment processes could not be easily identified.

Fraud risks included in the latest risk assessments are too high level and generic. For example, the latest risk assessments include one procurement risk category with three risk labels including tender manipulation, circumvention of procurement process and procurement variations in scope of work. However, within procurement there could be many sub-risks including – duplicated bidders, kickbacks, bribery, fake companies and personnel, etc. each requiring specific (and sometimes overlapping) detection and prevention mitigating actions.

Fraud-related pandemic risks were not included in the fraud risk assessment. As per the latest UN Board of Auditors report, in the United Nations, "*59 per cent of the entities declared that new risks of fraud and presumptive fraud arisen as a result of the pandemic. From them, 41 per cent stated that procurement risks and cyber security risks, were the main new threats observed; while 29 per cent declared that contractor risks and 18 per cent stated that payments/grants/loans risks were the main new fraud risks detected*." Specific guidance was provided during three webinar training sessions instructing field offices to carefully consider the impact of the COVID-19 pandemic.

The fraud risk assessments also include a column in which field offices can list key existing fraud controls. This helps the office to devise the residual risk score for each of the 19 standardized risks. Review of a sample of the fraud risk assessments showed that the controls listed were standard organizational controls that are available to all offices. They were generally not specific to the individual office, such as "evaluation committees", "quality assurance process", "monitoring visits" and "segregation of duties". If this is the preferred methodology for UN Women, it would be better to standardize the fraud controls as it has with the fraud risks to generate a risk and control map against which the risk scores are calculated. At the same time, the listed key controls do not include specific activities designed to detect and prevent fraud, making it a largely academic exercise with limited practical use.

Recommendation 6 (Medium):

The Director, SPRED to:

a) Develop a business case to enhance the online risk management system and database to conduct all risk assessments with adequate reporting and analytical capacities (considering options for off-the-shelf available applications or in-house application which might however require time and efforts).

b) Mandate risk assessments for business process/policy owners and, using the consolidated results, develop a specific fraud risk library that includes information about common fraud schemes and how they could be perpetrated, prevented and detected within UN Women's specific context (e.g., duplicated bidders, kickbacks, bribery, fake companies and personnel).

c) Provide offices and units with the ability to add their own specific risks to the fraud risk assessments. Manually entered risk information should be controlled to ensure proper data integrity so that risks can be analysed holistically.

Issue 6: Accuracy of fraud risk ratings

"Our risk assessment team evaluates the likelihood and significance of identified fraud risks based on historical information, known fraud schemes, and interviews with business process owners. Our management assesses the likelihood of a fraud risk's occurrence by determining instances in which the particular fraud has occurred in our organization in the past, the prevalence of the particular fraud risk in our organization's industry, and other factors." (ACFE Fraud Risk Assessment Scorecard)

The 73 field offices which conducted the fraud risk assessment generated average residual risk ratings across the 19 generic fraud risks as follows:

Table 3: Average residual risk ratings of field offices conducting fraud risk assessment

Average risk level	Number of field offices	Percentage of field offices
High	1	1%
Moderate	41	56%
Low	29	40%
Not complete	2	3%
Total	**73**	

Table 4 shows the data from the field office fraud risk assessments stratified by Corruption Perception Index and includes country information. The index ranks 180 countries and territories by their perceived levels of public sector corruption.

The audit compared field office risk ratings with the Corruption Perception Index: all but five of the offices had a CPI below 50;[4] and only one office rated itself as a high-risk country for fraud. Field offices could use the CPI index to align their risk assessments with the local context raised by CPIs (see Issue 5 on generic risk categories).

[4] As per the Transparency International website "the index, which ranks 180 countries and territories by their perceived levels of public sector corruption according to experts and businesspeople, uses a scale of zero to 100, where zero is highly corruption and 100 is very clean."

Table 4: Fraud risk assessment data stratified by the Corruption Perception Index (CPI)

CPI score	Risk rating				Regional, Country or Programme Presence Office
	H	M	L	N/A	
Below 25		9	2		Palestine, Somalia, South Sudan, Yemen, Sudan, Haiti, DRC, Afghanistan, Burundi, Iraq, Honduras
25 to 30	1	6	8	1	Chile, Guatemala, Lebanon, Mozambique, Tajikistan, Cameroon, Nigeria, Bangladesh, CAR, PNG, Uganda, Paraguay, Myanmar, Liberia, Malawi, Mali
31 to 35		8	6		Bolivia, Mexico, Pakistan, Kenya, ESARO, Kyrgyzstan, Niger, Nepal, Egypt, ROAS, Ukraine, Moldova, Bosnia and Herzegovina, FYR-Macedonia
36 to 40		9	10		El Salvador, ROAP, Vietnam, Albania, Kosovo, Cote d'Ivoire, Indonesia, Brazil, Ethiopia, Tanzania, Kazakhstan, Serbia, Columbia, Ecuador, India, Timor L'Este, Morocco, ECARO, Turkey
40 to 50		6	1	1	Argentina, China, Fiji, Tunisia/Libya, South Africa, WCARO, Senegal, Jordan
Above 50		3	2		Rwanda, Georgia, Barbados, ROAC, Uruguay
Total	**1**	**41**	**29**	**2**	

In its Meta-Synthesis Report on Results of the Field Office Audits (issued in Feb 2021), IAS noted "*One common issue was that fraud risks were not sufficiently identified and addressed in a sustainable manner, regularly reviewed by the FO [Field office], and their mitigating actions were not updated…. When reviewing the risks in detail, IAS found the risks identified were frequently brief and high-level, rather than specific or used in an effective way to prevent and detect wrongdoing*."

The 2021 risk assessment was meant to address some of the issues identified in earlier

audits. The ERM function has started to analyse the fraud risk scores reported by offices, taking into account not only the CPI index, but other relevant internal and external criteria. It also reviewed the completeness, existence and accuracy of reported fraud risks by individual offices. However, ERM function does not have the capacity, or the perspective required to review the completeness of fraud risk registers in their entirety. This is also true of Regional Offices, which do not have a clear role in the process. The ERM function could develop a quality assurance process to be used by Regional Offices to ensure that fraud risk scores are appropriate and useful decision-making tools for management.

Recommendation 7 (Medium):

The Director, SPRED to:

a) Devise a procedure for the meta-analysis of key fraud risks analysed by offices and regions.

b) Formalize a quality assurance process for fraud risk assessments, including the existing fraud risk meta-analysis.

c) Coordinate implementation of the process with headquarters risk focal points and Regional Offices.

Issue 7: Fraud risk assessment reports

"Our fraud risk assessment team includes all appropriate levels of management and internal and external sources to assess fraud throughout the organization. Management, senior management, business unit leaders, and significant process owners participate in the risk assessment seeing as they are ultimately accountable for the effectiveness of our organization's fraud risk management efforts. Our fraud risk assessment team shares its fraud risk identification information with the board and solicits feedback from them. Our board assesses the implications of its own processes on fraud risk and considers how its policies may create pressures and incentives to commit fraud." (ACFE Fraud Risk Assessment Scorecard)

The Risk Management Policy establishes roles and responsibilities for risk management across the three lines of defence. As per the policy, the headquarters risk management specialist *"consolidates, disaggregates and reports on Risk data across all UN Women Risk Entities in order to determine a Risk profile for the organization and prepare Risk Management reports at various levels as required".* The policy also notes that *"an annual reporting process will be undertaken by the HQ Risk Management Specialist (working with the Regional Risk Focal Points). This report will be provided to the Risk Management Committee as well as to the Advisory Committee on Oversight and will provide an update on the effectiveness of the Risk Management Framework, against the agreed upon standards and key performance indicators related to Risk Management."*

The above roles and responsibilities were established in the latest version of the Risk Management Policy, promulgated on 15 October 2020. This represents a significant organizational improvement and involved considerable change management activities to operationalize the updated policy.

Fraud risk reporting to the Risk Management Committee has not yet begun. As the policy was updated in 2020, the first year of reporting is 2021, which was not complete at the time of audit. A draft version of the Risk Assurance Framework document is pending approval by the Risk Management Committee, most likely in Q3 2021. Once the framework is finalized, the first report will be prepared for 2021. The JIU conducted a review of "*Fraud Prevention, Detection and Response in United Nations System Organizations*" in which UN Women was asked to *"present an annual report to governing bodies on anti-fraud activities".* This recommendation was marked as complete; however, fraud risk reporting was not completed.

As discussed in Issue 5, part of an analysis of key fraud risks in field offices was performed, but not reported to management or acted upon. Headquarters and business process owner assessments are planned for Q3 and Q4 2021. An appropriate risk reporting mechanism should also cover the analyses to be performed, how they are to be reported and to whom.

Recommendation 8 (Medium):

The Director, SPRED to operationalize fraud risk reporting to the Risk Management Committee, ACO and Executive Board.

D. FRAUD POLICIES AND CONTROL ACTIVITIES

Issue 8: Strengthening fraud detection and prevention measures

"We use data analytics procedures to examine journal entries for suspicious transactions…" "We use data analytics procedures to identify anomalous relationships among people, organizations and events. We proactively consider how certain fraud schemes may result in identifiable types of transactions or trends so that we can design and implement our data analytics procedures accordingly." (ACFE Fraud Control Activities Scorecard)

"The design and implementation of our fraud control activities represent a coordinated effort by senior management and the support of personnel representing all significant business processes across the organization. Our control activities adequately mitigate the risk of fraud in accordance with our organization's specific risk tolerance. We have transaction controls in place that mitigate transaction processing risks in our organization's business processes by testing for completeness, accuracy and validity. We perform background checks on prospective and existing suppliers, customers, and business partners to help us identify any issues of financial health, ownership, reputation, and integrity that represent a risk to our organization." (ACFE Fraud Control Activities Scorecard)

Overall, fraud preventive and detection controls in UN Women need to be improved. First, policy design should focus on anti-fraud and anti-corruption provisions. In Issue 1, IAS referred to misalignment of the Anti-Fraud Policy with operations-related policies such as HR, travel and others. The policies generally do not include references to anti-fraud issues because there is no corporate requirement to consider this during policy design. IAS makes recommendations in this report to strengthen policy design based on fraud risk assessments conducted by business process owners, which will significantly improve the adequacy of policies.

Second, compliance with policies should be enhanced by individual unit's fraud risk assessments and the specific anti-fraud mitigating actions for each office and local context.

Finally, addressing culture and accountability in terms of integrity, awareness of anti-fraud and anti-corruption actions would strengthen the state of preventive and detection fraud controls. This would culminate in the Statement of Internal Controls prepared by management on an annual basis.

Fraud detection

In 2016, the JIU conducted an inspection of Fraud Prevention, and Detection, Response in the UN System (JIU/REP/2016/4). Recommendation 10 noted *"The executive heads of the United Nations system organizations should ensure that proportionate fraud prevention and detection capabilities are an integral part of automation systems' functionalities, including automated activity reports and data-mining modules in their respective enterprise resource planning systems (ERPs)."* UN Women considers this recommendation implemented, but the audit found that gaps remained. For example, the UN Women Anti-Fraud Policy does not include provisions on the use of data analytics to detect fraud, nor is it clear who should be responsible for a data analytics and fraud monitoring (which is yet to be developed).

Many of the fraud prevention and detection capabilities of the UN Women ERP system are not set up and used. While the segregation of duties function is operational and forms part of any fraud prevention strategy, reporting on exceptions or identifying other red flags are not yet conducted as fraud detection efforts (as identified by the 2020 IAS meta-synthesis of field office audits and the 2020 audit of policy cycle management). Many of the types of data needed to track exceptions (e.g., method of procurement – competitive, direct, etc.) are not captured within the system. While some policies (e.g. procurement, programme partners) generally include key controls to address fraud risks across key processes, the controls and related exceptions are not tracked or monitored in the system, making it difficult to conclude on their overall effectiveness.

UN Women has a range of systems and databases that could be used to monitor fraud risk. For example, data in the e-procurement system could help to identify similar,

identical or related bidders for a contract. It could also analyse trends such as repeated winners, and support analysis of whether sufficient market research had been conducted to support proper competition. This is also true for data housed in other systems such as Atlas, and OneApp modules such as RMS and others.

If controls are automated in the incoming #NextGenERP and reporting tools are available to identify red flags and exceptions, both risk and policy owners will be able to conduct effective monitoring and oversight.

Fraud prevention

As noted above, UN Women needs to strengthen and mature its anti-fraud culture (Issue 4), risk management process (Issue 5) and managerial and personnel accountability (Issues 3, 9 and 10). This will help to create a stronger fraud prevention culture and environment.

Several thematic audits also identified additional preventative controls that could be developed. Despite strong progress made, UN Women could significantly improve controls over programme partners. The organization could better monitor and enforce performance of proper capacity assessments to track partner performance improvements and maturity. UN Women could also review and strengthen the conditions under which cash is advanced to partners, ensuring use of a risk-based approach linked to partner capacity and prior performance.

At the time of audit, Atlas did not have controls to enforce implementation of delegation of authority limits for approvers. For example, there is nothing to prevent someone with a procurement or finance delegation of authority up to US$ 50,000 approving transactions for more than that in Atlas if they have been assigned the 'Senior Manager' profile. It is also possible to approve a transaction that relates to yourself, for example a transaction reimbursing expenses or paying daily subsistence allowance. UN Women is in the process of adopting a new ERP system (led by UNDP), but it is still unclear whether the new ERP will include built-in automated budgetary and financial controls.

UN Women does not have an automated mechanism for managing delegations of authority. Personnel with a delegation of authority receive a written letter (in electronic form) notifying them of their delegation of authority and their responsibilities therewith. There is no system for tracking these delegations of authority or applying limits to systems in which transactions can be made (as mentioned above).

IAS analysis indicates that the e-procurement system is not being used for all procurements. Sixty-nine procurements advertised on the United Nations Global Marketplace (UNGM) did not appear to have a corresponding case raised in the e-procurement system. The system was developed partly to automate key controls; however, because offices are not using it, they may be exposing the organization to fraud risks in the procurement process. It is possible to deliberately not use the system to circumvent key fraud controls.

Recommendation 9 (Medium):

The business process owner and Director, DMA to:

a) As a part of the JIU recommended Statement on Internal Control, consider developing individual manager accountability statements including confirmation that fraud risks and related controls are regularly.

b) Consider how best to utilize data analytic techniques to detect and prevent potential fraud. Based on this, devise a fraud data analytics strategy.

c) Develop a detection and enforcement mechanism to ensure use of key controls such as the e-procurement system.

d) Take the opportunity of the new ERP to set up in-system controls and an exception reporting mechanism.

E. FRAUD INVESTIGATION AND CORRECTIVE ACTION

Issue 9: Improving the fraud investigation mechanism

"Our fraud investigation and response system includes protocols for: updating a central repository for allegations and complaints; maintaining anonymity or confidentiality of involved individuals, except as is necessary to investigate; initially evaluating the allegations to determine if an investigation is warranted and the appropriate degrees of urgency; notifying employees regarding document preservation and securing data systems; if necessary, engaging independent counsel and forensic accounting support;

conducting the investigation while controlling and safeguarding evidence; reporting the results in the appropriate format (oral summary of key points or comprehensive written report with exhibits); following policies regarding retention of reports, documents, work papers, and other information; assessing root causes and initiating mitigating processes and controls." (ACFE Anti-Fraud Playbook) "Promoting and supporting open communication and tips is vital to ensuring the effectiveness of reporting mechanisms and is a key element of an effective anti-fraud culture." (ACFE Anti-Fraud Playbook)

Receiving and processing allegations

OIOS is fully responsible for receiving the allegations of principal types of wrongdoing (being the formal reporting channel), their preliminary assessment and, if assessed as warranted, further investigation.

UN Women (through IEAS) does not have direct real-time access to detailed allegation information and relies on OIOS quarterly statistics reports as well as its information requests and occasional updates. Allegations are recorded in the OIOS Case Management System as they are received, and then reflected in the quarterly statistics provided to UN Women.

Currently, OIOS does not have direct access to UN Women corporate systems to collect or verify information and depends on responses to its information requests by IEAS or other UN Women offices and personnel, OIOS case statistics may lack some details (for example, the funding source(s) of the presumptive fraud in question, although IAS also acknowledges that often this might be difficult to identify). In some cases, as per their agreements with UN Women, the Entity (IEAS) has to inform (even briefly) relevant donors about alleged fraud if their funding is involved.

OIOS commenced 43 investigations from January 2018 until June 2021. Of the 25 cases that were completed by 30 June 2021, the average time from receiving allegation to submission of report to UN Women was 347 days. The remaining 18 cases have been open for an average 372 days. Other UN funds and programmes experienced average closure times of between 5 and 12 months. IAS understands the long timelines may be due to OIOS workload, priority of higher profile non-UN Women investigations, greater complexity to investigate for another UN organization (i.e. UN Women, to whose systems, data and personnel OIOS has does not always have real-time access), investigation quality standards and assurance (to prevent legal disputes of investigation findings), and COVID-19 related travel and office work restrictions (e.g. access to personnel, external parties and documents) equally for OIOS, investigation subjects, witnesses and information providers. OIOS has also indicated that their investigations experience shows issues within UN Women with leadership, integrity and 'tone from the top' among some UN Women managers, and that UN Women personnel generally do not cooperate well (delay cooperation) with OIOS investigations.

OIOS invoiced UN Women US$ 128,152 for investigations completed in 2020 and US$ 160,056 for those completed in 2019 on a cost recovery basis. OIOS bills UN Women based on completed investigations. Other services that it provides, such as case intake and assessment, are not directly costed and billed. In comparison, JIU analysed the resources of UN organizations' investigation functions as part of its larger review (JIU/REP/2020/1). The average investigation unit budget for the other funds and programmes (UNDP, UNFPA, UNHCR, UNICEF, UNOPS, UNRWA and WFP) was US$ 2.51m. The lowest budget was US$ 0.9m and the highest was US$ 6.1m.

The end-to-end investigation process is currently under-funded and is being subsidized by other budgets. Moreover, longer investigations also incur other actual and indirect costs. For example, in some cases affected persons or investigation subjects had to be put on long-term paid leave (there was an instance in which this had been ongoing since 2019) or had to be reassigned to other duties (this became more feasible with remote work arrangements but was often difficult for in-person work, i.e., usually it was not possible to move the person to another duty station). Offices with already very limited resources also needed to hire temporary replacements for these positions. In addition, HR, Legal, IEAS and other management units spend many hours dealing with these issues. The affected persons and some subjects have at times raised concerns about the long investigations and their impact on their work, career, health and wellbeing. UN Women senior managers also communicate such concerns to IEAS (especially, where the subjects may be in management positions).

There may also be situations where subjects have left the organization before investigations are completed. Moreover, lost funding opportunities and reputational issues were mentioned as another consequence of prolonged investigations (though IEAS notes in one case this was linked to UN Women's previous investigations provider – UNDP). A swifter case resolution process could help to reduce these large backstage costs and unproductive work environment issues for the organization.

Handling allegations assessed as not requiring OIOS investigation

Some matters reported may not warrant a full investigation because the evidence is clear enough for management to take a management action, in principle, or a disciplinary action based on a short investigation. The matter may also not require serious disciplinary action and could be dealt with through reprimand, financial recovery or other disciplinary measure. However, currently all the investigations have to go through OIOS full-scope investigations which take considerable time on average (see above) because the current UN Women Legal Policy for Addressing Non-Compliance with UN Standards of Conduct does not give the authority to discharge responsibility for investigations to another office than OIOS, as well as does not foresee imposing disciplinary measures without an investigation. Despite that, OIOS does refer some allegations to UN Women management when they assess that an investigation is not warranted (or in some cases, needed) based on preliminary review.

Moreover, the legal policy also does not address conduct which may be referred to as "unsatisfactory" rather than misconduct. Such unsatisfactory conduct may not require an expensive and time-consuming investigation and could be dealt with through performance management and/or a disciplinary procedure. For example, UN Secretariat Administrative Instruction ST/AI/2017/1 establishes a distinction between unsatisfactory conduct that rises to the level of misconduct and unsatisfactory conduct that does not; and recommends different courses of action for each – in short, disciplinary measures versus administrative measures and other management actions.

Lastly, other matters reported may pertain to third parties and implementing programme partners who work with UN Women. While some matters would warrant a full investigation, others may require other actions by management which could, in principle, be undertaken without the completion of an investigation report. This also poses a challenge as the UN Women Legal Policy for Addressing Non-Compliance with UN Standards of Conduct does not provide a specific legal construct for addressing vendor and partner misconduct. Such matters could be addressed through reference to vendor contracts or partner agreements, and related policies, which need to be fully aligned and clarified (including on procedure for referral of criminal activities to national authorities).

The above-mentioned lower risk, lower exposure, less grave or potentially straightforward allegations could be potentially investigated by independent, trained and capacitated professionals outside of the current set-up with OIOS as the only accepted formal investigation function. Certain investigations could also be undertaken by other competent UN offices qualified in specialized investigations, for example UNDSS or Special Investigation Units of UN field missions (as is the legal frameworks of some other UN organizations). However, UN Women's policy and procedures would need to be updated to accept and accommodate such approaches.

Other UN entities provide for the possibility that misconduct can be addressed by management without launching a fully-fledged, formal investigation. While OIOS has overall authority for UN Secretariat investigations it can discharge this responsibility to other offices. As stated in its investigation manual "the expertise of professional investigators is required for complex fraud or criminal activities, while a lay panel of staff members may appropriately deal with cases that review behavioural problems." UNICEF's Policy on the Disciplinary Process and Measures states "conduct that is not of a sufficient gravity to amount to misconduct may be addressed by the responsible manager(s) through administrative measure(s) or managerial action." In addition, it states that "if the report contains sufficient information that could sustain, as a matter of law, a finding of misconduct without the need for an investigation, OIAI shall transmit the report to the Deputy Executive Director, Management, for his/her assessment." UN Women's Legal Policy for Addressing Non-Compliance with UN Standards of Conduct has a similar section on "non-disciplinary measures" for subjects of investigations.

Based on analysis of the significant issues identified, potential solutions, in IAS view, UN Women's legal framework should be updated to provide the authority, resources and processes for (partial or full) internal management of some investigation activity (if properly resourced).

Triage of allegations

An organization should have an independent and properly resourced case intake function that reviews and channels issues to the most appropriate body to investigate or identify facts so that appropriate action can be taken. Currently, OIOS performs this function for complaints received through the formal investigation reporting channel. As OIOS charges UN Women based on cost-recovery for completed investigations, this service is not explicitly billed. Some allegations are closed by OIOS after their assessment because of lack of evidence and credibility and/or are referred to UN Women for information and potential management action (where OIOS decides that

the matter is within purview of UN Women management and an investigation is not an appropriate tool to address it). From January 2018 to June 2021, among 112 closed cases, OIOS closed 53 (47%) "for information" and referred 34 (30%) for UN Women management action. OIOS have indicated however, that it has been exploring better funding from UN Women for its services and a request for better funding of the investigation process is being finalized.

UN Women can continue using OIOS to receive and assess formal complaints received. If UN Women updates its posture and policy so that lower risk, lower exposure, less grave or potentially straightforward allegations could be potentially investigated by others, then OIOS could channel such allegations accordingly.

As an alternative, UN Women could also consider to task IEAS as the office designated to support investigation activities (and if resourced for this task) to coordinate investigation grievance mechanisms. This could provide for more real-time information. After a complaint is received, it could be triaged based on established protocols and delegation of authority.

Recommendation 10 (High):

The UN Women Executive Office, in consultation with IEAS, Legal, HR and OIOS, to:

a) Consider whether to continue with the current outsourced case intake and assessment measures, or to potentially establish internal triage protocols with clear criteria where formal grievances are reviewed and referred to the appropriate function (e.g., OIOS, IEAS, HR, PSMU, HQ/Regional, Country Office management, UN Ethics Office etc.) with due consideration to the nature, complexity, credibility and materiality of the complaint, and the need for any whistle-blower protection;

b) Update the legal policy framework for UN Women that codifies its investigative, disciplinary and non-disciplinary (including referrals to national authorities) protocols for staff, other personnel and third parties (e.g. vendors, programme partners), as well as investigation outsourcing arrangement, addressing fact-finding/investigation roles to be potentially performed by independent UN Women parties and what will be outsourced; and

c) Update the investigations portion of the IEAS charter as relevant.

Issue 10: Strengthening the fraud investigation function

"Establish enterprise-wide fraud investigation and response protocols. These protocols should align with the established FRM governance structure, as they are important inputs to your organization's overall fraud response plan. In addition, these protocols should define roles and responsibilities across the investigative process, including who is responsible for conducting investigations." (ACFE Anti-Fraud Playbook)

"Our organization ensures that any reasonably suspected or known violation, deviation, or other breach of code of conduct, fraud, or corruption is dealt with in a timely and effective manner." "The performance metrics we use to evaluate the efficiency and effectiveness of our investigation process are tailored to the scope, scale, and complexity of the fraud investigation at hand." "Our organization stresses the importance of having a documented process in place by which allegations of fraud are to be consistently captured, assessed, and responded to in a timely manner." (ACFE Fraud Investigation and Corrective Action Scorecard)

Monitoring the performance of the investigative function

JIU conducted a review of "*Fraud Prevention, Detection and Response in United Nations System Organizations*" in 2016 which included a recommendation for ensuring the investigative functions have KPIs for conduct and completion of investigations. While this recommendation was marked implemented by UN Women, the organization does not have any formal KPIs for tracking investigations progress. The Memorandum of Understanding between UN Women and OIOS (Annex II) only indicates *"timely fashion"* and *"informing on significant delay"* as KPIs for OIOS investigations.

The UN Women Advisory Committee on Oversight in its address to the UN Women Executive Board's 2021 annual session noted "the timeframes for receipt of reports from OIOS on completed investigations is fairly long but is not out of line with those of other UN agencies according to data from a 2020 Joint Investigation Unit (JIU) report. The ACO will want focus in future work on whether these time frames pose any issues for UN-Women and whether improvement is possible." The ACO noted that UN-Women

should carefully consider the risks arising from the inability of IEAS to conduct certain fraud prevention work because of insufficient resources. In 2020-2021, the Director, IEAS and Chief, IAS spent about 10-20 per cent of their time on investigation matters, and an IAS Audit Specialist (P4 level) spent 30 per cent of his time on them, with occasional support also from other Audit Specialists. However, IAS did neither have such responsibilities in its Charter, nor it had a budget for this purpose. In September 2021, IAS used its operational budget to also hire a UN volunteer to support investigation matters.

Recommendation 11 (High):

The UN Women Executive Office, together with Chief, IAS, Legal and Director, IEAS to:

a) Ensure that key performance indicators are devised and tracked that set expected investigation processing times and escalation in the event that cases take long to resolve.

b) Ensure the Director, IEAS, who is involved in supporting the investigation function is appropriately resourced.

F. FRAUD MONITORING

Issue 11: Nature, scope, frequency and measurement of anti-fraud monitoring

"Our organization's fraud risk management monitoring plan targets our areas of highest fraud risk. Our monitoring activities focus on these aspects of the analysis performed: "Why," "who," "what," "where," and "what's next?" Our ongoing monitoring activities include data analytics procedures used to form conclusions about information collected. We document our plan, approach, and scope for monitoring our organization's fraud risk management program. Our organization's plan for monitoring our fraud risk management program includes a balance of ongoing and separate evaluations deemed appropriate to assist management in its evaluation of whether each of the five principles of fraud risk management is present and functioning in its fraud risk management program." (ACFE Fraud Risk Management Monitoring Scorecard)

At the time of this audit, no formal mechanism was in place to monitor the effectiveness of the anti-fraud programme at UN Women, with KPIs to be measured and reported over time. Moreover, the Anti-Fraud Policy does not establish a fraud risk monitoring programme that targets the Entity's areas of highest fraud risk. The Anti-Fraud Policy needs operationalization through an action plan which should be monitored for effectiveness (see Recommendation 3). Such a plan would establish who is responsible for conducting anti-fraud monitoring activities within UN Women, the monitoring of these activities and how the effectiveness of the anti-fraud programme is measured, e.g. regularity and validity of fraud risk assessments, communication and training, culture and tone-at the top.

The Risk Management Policy establishes roles for monitoring all risks identified by the ERM process. However, fraud monitoring is not specifically discussed in the policy. The draft Risk Assurance Framework, which facilitates reporting on agreed-upon risk maturity indicators and metrics (including completion of fraud risk assessments), was pending approval by the Risk Management Committee at the time of audit. IAS believes this arrangement could be an organic placeholder for the anti-fraud programme's maturity indicators and metrics to be included in the Risk Assurance Framework.

According to the ACFE, "*monitoring and periodic evaluations should cover the full spectrum of your Fraud Risk Management program, and at a high level include two key steps: (1) implementing monitoring and evaluation activities and (2) using the results to improve your FRM program*." Instead of just reviewing the outputs from the anti-fraud programme (number of cases, number of referrals, types of disciplinary action, etc.), UN Women needs to measure the outcomes of the programme, for example how fraud awareness has improved over time.

Monitoring activities should also inform adjustments to the anti-fraud programme based on new information, such as when UN Women enters a new business area (e.g. cash payment modalities) or when new types of fraud schemes emerge (e.g. with respect to cybersecurity). Deficiencies in the programme should be periodically identified and addressed.

Recommendation 12 (Medium):

The business process owner to develop an anti-fraud monitoring mechanism to assess the effectiveness of the Anti-Fraud Policy. This should establish the responsibility of individual policy owners to monitor their policies and provide feedback to the anti-fraud business process owner. This should include establishment of appropriate measurement criteria based on UN Women's fraud risk tolerance and organizational outcomes. It should also include a mechanism for communicating and rectifying issues with the anti-fraud programme, and capture lessons learned.

V. RECOMMENDATIONS AND MANAGEMENT ACTION PLAN

Issue	Recommendation	Process	Responsible Unit	Priority	Action Plan	Implementation date
Issue 1: Roles and responsibilities	1. BRC in its role as Risk Management Committee to reassign responsibility from IEAS to an appropriate business process owner with the clear accountability and accompanied sufficient authority, capacity and resources to implement the overall Anti-Fraud Programme and coordinate its governance, fraud risk assessment, internal control system, and monitoring with the necessary support and engagement from other contributing business process owners along the three lines of defence model.	Fraud Risk Governance	Business Review Committee to decide	High	Pending decision of the Business Review Committee	To be agreed
	2. The business process owner to revise the Anti-Fraud Policy in terms of roles and responsibilities, and its ownership in line with the three lines of defence model. In particular: a) Assign the key contributors to the policy, including senior management or specific key business process owners, IEAS (in its capacity as the designated office in supporting investigation-related activities), and the oversight and advisory role of the Advisory Committee on Oversight. b) Reassign responsibility for fraud risk monitoring across the three lines of defence in the Anti-Fraud Policy, ensuring consistency with related policies and appropriate legal instruments. c) Establish a formal matrix of responsibility within the Anti-Fraud Policy for the various anti-fraud activities that refers to specific roles, functions, units and divisions. d) Request that the PPG function include in the PPG Framework Policy a requirement for key policies, when developed or reviewed, to specifically include controls to prevent, detect and correct fraud with reference to the overarching Anti-Fraud Policy. e) Request that policy owners take stock of key anti-fraud activities foreseen in their policies and, based on this exercise, align the activities with the Anti-Fraud Policy, either directly or through referral to those policies within their own fraud sections.	Fraud Risk Governance	Business Process Owner	High	Pending decision of the Business Review Committee	To be agreed
	3. The business process owner to coordinate with other key contributors (including HR, PSMU, Legal and IEAS) and develop an action plan with	Fraud Risk Governance	Business Process Owner	High	Pending decision of the Business Review Committee	To be agreed

	clear objectives, roles, resources and activities to operationalize the Anti-Fraud Policy, once it has been revised, to address the issues raised in this report. Moreover, to include in the Anti-Fraud Programme action plan an analysis performed by respective business process owners of risks, controls and key gaps. Implementation of the action plan should be reported to senior management and governing bodies. Also, addressing Issue 4 below, the business process owner to include a set of actions to improve UN Women's anti-fraud culture, awareness, training and communications in the anti-fraud programme action plan.					
Issue 2: Aligning definitions of fraud and misconduct	4. The business process owner and Director, SPRED to: a) Include UN Women's zero tolerance principle, risk tolerance and appetite to fraud and corruption in the Anti-Fraud Policy and Risk Management Policy and Procedure. b) Establish a mechanism to ensure other business process owners align the definitions of fraud throughout their relevant PPG. c) Consider expanding definitions in the Anti-Fraud Policy to include topics such as corruption and other unethical practices.	Fraud Risk Governance	Business Process Owner, SPRED	Medium	a) SPRED/ ERM will work in tandem with BPO to revise the Anti-Fraud Policy and Risk Management Policy b) SPRED/ PPG to support BPOs with aligning definitions of fraud across PPGs in connection with document revisions/ development of new documents	Q3-2022 *(Subject to identification of BPO)* Q4-2022
Issue 3: Fraud and corruption training and awareness	5. The business process owner to: a) Follow up on the pending request to improve the system for tracking the completion of mandatory training, and develop a mechanism to hold managers accountable for not ensuring all personnel complete the training. Institute accountability measures for non-completion of mandatory training, especially for senior personnel and those with budget management responsibilities. b) Revise and align the mandatory training completion deadlines, ideally making them mandatory within the first 30 days c) Develop annual refresher training. d) Conduct periodic user surveys to assess the effectiveness of training materials. e) Develop fraud reporting and fraud case handling training for managers to be delivered as part of manager induction and including periodic refreshers.	Fraud Risk Governance	Business Process Owner	Medium	Pending decision of the Business Review Committee	
Issue 5: Strengthening fraud risk assessments	6. The Director, SPRED to: a) Develop a business case to enhance the online risk management system and database to conduct all risk assessments with adequate reporting and analytical capacities (considering options for off-the-	Fraud Risk Assessments	SPRED	Medium	a) SPRED will review and modify existing business case to address this finding accordingly and standby to present the business case to the ICT Governance Board at such time as the Board agrees. b) Included in the current Risk Assessment Guidance and Risk	2023

	shelf available applications or in-house application which might however require time and efforts). b) Mandate risk assessments for business process/policy owners and, using the consolidated results, develop a specific fraud risk library that includes information about common fraud schemes and how they could be perpetrated, prevented and detected within UN Women's specific context (e.g., duplicated bidders, kickbacks, bribery, fake companies and personnel). c) Provide offices and units with the ability to add their own specific risks to the fraud risk assessments. Manually entered risk information should be controlled to ensure proper data integrity so that risks can be analysed holistically.				Register Template is an instruction that offices may include additional risks applicable to their context. In line with the system enhancements business case, SPRED will review how to ensure proper controls so manually entered risks can be captured in the ERM system. c) A Fraud Risk Management training is planned for HQ BPOs during Q4-2021. Following the training, BPOs will conduct fraud risk assessments to be informed both by contextual analysis as well as the entity-level Fraud Risk Assessments conducted by UN Women Regional Offices and Country Offices during Q2-Q3-2021.	
Issue 6: Accuracies of fraud risk ratings	7. The Director, SPRED to: a) Devise a procedure for the meta-analysis of key fraud risks analysed by offices and regions. b) Formalize a quality assurance process for fraud risk assessments, including the existing fraud risk meta-analysis. c) Coordinate implementation of the process with headquarters risk focal points and Regional Offices.	Fraud Risk Assessments	SPRED	Medium	a) SPRED will prepare a meta-analysis of fraud risks building on the outcomes of the unit-level Fraud Risk Assessments. b) A pilot quality assurance process commenced in Q3 2021 for field offices and this process will be formalized, also drawing on findings from this report. c) The quality assurance process will include roles/ responsibilities for relevant BPOs at the HQ level and Regional Office risk focal points.	2022
Issue 7: Fraud risk assessment reports	8. The Director, SPRED to operationalize fraud risk reporting to the Risk Management Committee, ACO and Executive Board.	Fraud Risk Assessments	SPRED	Medium	Following the completion of the quality assurance of Fraud Risk Assessments, meta-analysis of key fraud risks, and engagement with HQ BPOs, a report will be prepared and presented to the Risk Management Committee on fraud risks.	Mid-2022
Issue 8: Strengthening fraud detection and prevention measures	9. The business process owner and Director, DMA to: a) As a part of the JIU recommended Statement on Internal Control, consider developing individual manager accountability statements including confirmation that fraud risks and related controls are addressed regularly. b) Consider how best to utilize data analytic techniques to detect and prevent potential fraud. Based on this, devise a fraud data analytics strategy. c) Develop a detection and enforcement mechanism to ensure use of key controls such as the e-procurement system. d) Take the opportunity of the new ERP to set up in-system controls and an exception reporting mechanism.	Fraud Policies and Control Activities	Business Process Owner, DMA	Medium	Pending decision of the Business Review Committee	To be agreed
Issue 9: Improving the fraud	10. The UN Women Executive Office, in consultation with IEAS, Legal, HR and OIOS, to:	Fraud Investigation	Executive Office	High	Pending decision of the Business Review Committee	To be agreed

investigation and grievance reporting mechanism	a) Consider whether to continue with the current outsourced case intake and assessment measures, or to potentially establish internal triage protocols with clear criteria where formal grievances are reviewed and referred to the appropriate function (e.g., OIOS, IEAS, HR, PSMU, HQ/Regional, Country Office management, UN Ethics Office etc.) with due consideration to the nature, complexity, credibility and materiality of the complaint, and the need for any whistle-blower protection; b) Update the legal policy framework for UN Women that codifies its investigative, disciplinary and non-disciplinary (including referrals to national authorities) protocols for staff, other personnel and third parties (e.g. vendors, programme partners), as well as investigation outsourcing arrangement, addressing fact-finding/investigation roles to be potentially performed by independent UN Women parties and what will be outsourced; and c) Update the investigations portion of the IEAS charter as relevant.	and Corrective Action				
Issue 10: Strengthening the fraud investigation function	11. The UN Women Executive Office, together with Chief, IAS, Legal and Director, IEAS to: a) Ensure that key performance indicators are devised and tracked that set expected investigation processing times and escalation in the event that cases take long to resolve. b) Ensure the Director, IEAS, who is involved in supporting the investigation function is appropriately resourced.	Fraud Investigation and Corrective Action	Executive Office	High	Pending decision of the Business Review Committee	To be agreed
Issue 11: Nature, scope, frequency and measurement of anti-fraud monitoring	12. The business process owner to develop an anti-fraud monitoring mechanism to assess the effectiveness of the Anti-Fraud Policy. This should establish the responsibility of individual policy owners to monitor their policies and provide feedback to the anti-fraud business process owner. This should include establishment of appropriate measurement criteria based on UN Women's fraud risk tolerance and organizational outcomes. It should also include a mechanism for communicating and rectifying issues with the anti-fraud programme, and capture lessons learned.	Fraud Monitoring	Business Process Owner	Medium	Pending decision of the Business Review Committee	To be agreed

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.

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