United Nations System **2 October 2020**

CEB/2020/HLCM/20

CEB
Chief Executives Board for Coordination

High-Level Committee on Management (HLCM)

Cross-functional Task Force on Risk Management

Guidance Notes
Managing Fraud Risk

(HLCM 40th Session, 13 October 2020)

UNITED NATIONS SYSTEM

Table of Contents

1. Introduction

1.1 Background and purpose of this paper

At its 39th session in March 2020, the High-Level Committee on Management (HLCM) mandated the Cross-Functional Task Force on Risk Management (hereafter 'the Task Force') to develop guidance for UN organizations on how to best manage fraud risk. This document is intended to focus on three priority area of Managing Fraud Risk, as outlined below.

Managing fraud and corruption risk is a continuous and critical exercise. The increased rate of fraud and corruption over the past years and more recently the increased risk of fraud during the Covid-19 pandemic highlight the importance of having a strong and comprehensive Anti-Fraud/Anti-Corruption (AFAC) function across each UN Agency, which is also in line with the recommendations provided by the Joint Inspection Unit (JIU) in their 2016 report on Fraud Prevention, Detection and Response in UN Systems Organizations. This paper, along with its annex, provides an overview of key AFAC-related topics noted by the Task Force. Information was gathered through a comprehensive survey conducted among the HLCM Cross-Functional Task Force on Risk Management participants, which received 18 responses. Further benchmarking informed this paper on current practices within the UN System, noting consistencies, but also highlighting areas where further harmonization may be beneficial.

1.2 Intended audience and assumptions

This document has been developed for all persons involved in preventing and managing the risk of fraud and corruption including HLCM members, directors, risk specialists, and other staff. It is not a technical document, but rather focuses on practical advice. Most of the proposals can be implemented by all organizations; some however (such as a fraud risk assessment) may require a stronger supporting infrastructure of risk management policies, procedures and practices, i.e. at least a "developing stage" in the Reference Maturity Model.

2. Overview of Fraud and Fraud Risk Focus Areas

2.1 Fraud defined

The HLCM agreed the definition of Fraud[1] as “Any act or omission whereby an individual or entity knowingly misrepresents or conceals a fact (a) in order to obtain an undue benefit or advantage or avoid an obligation 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.” Organizations may have their own definition.

2.2 Fraud in context

Fraud is inherently a hidden crime and only a small part of potential fraud losses will be discovered. In their 2016 report[2], the JIU noted “In broad terms, the public and private sector average is in the range of 1 to 5 per cent of total revenue, whereas it is in the range of 0.03 per cent for the United Nations system. In other words, underreporting and/or non-detection in the United nations system could be significant and endemic.”

Considering the widespread view that most fraud goes undetected, organizations should improve their understanding of the nature, types and causes of fraud that may be employed by fraudsters. Donors increasingly expect a transparent dialogue regarding fraud exposures and losses, which means being aware of the fraud losses that they face and counter fraud strategies that they adopt. Fraudsters were quick to exploit vulnerabilities resulting from the Covid-19 pandemic, and organizations should be ready to prevent, detect and respond to increasingly sophisticated fraudulent schemes.

It is helpful to consider fraud policy holistically, and not as an isolated or ‘siloed’ area. It is linked to error, waste and IT security and many of the anti-fraud mechanisms should also be used to support other areas of misconduct such as sexual exploitation and abuse, and forced labor. Joining up counter-fraud strategy is likely to produce synergies, especially in reinforcement mechanisms.

[1] This definition of fraud was adopted by the UN High Level Committee on Management (HLCM) at its Thirty-Third Session in March 2017 (see CEB/2017/3).
[2] JIU_REP_2016_4

2.3 Fraud Risk Focus Areas

All proposed focus areas were rated by the Task Force to garner a consensus on their relative importance. The following focus areas were prioritized and reviewed in depth. This document aims to provide an overview of leading practices in these respective areas for UN Agencies to consider and apply as appropriate for their context.

1. AFAC Policy and organizational responsibilities;
2. Prevention and detection measures;
3. Fraud response and sanctions.

The following focus areas were reviewed at a high level, including through the survey (summarized in the Annex, full results available on the Risk Management Information Sharing Platform), and may be examined further in future.

4. Toolkits and training;
5. Assessing exposure to fraud and corruption;
6. Reporting fraud.

3. AFAC Policy and Organizational responsibilities

In order to help combat fraud and corruption within the UN system, all organizations confirmed that they have a policy related to Anti-Fraud/Anti-Corruption (AFAC), the majority of which have clear linkages with that organization's Enterprise Risk Management (ERM) Framework. The AFAC policy, generally approved by the head of the organization or the governing body, clearly outlines the applicability of the policy (scope) and establishes definitions of fraud, corruption, and other prohibited practices, as well as roles and responsibilities of internal and external stakeholders related to fraud and corruption. Additionally, most of the sampled policies stated that the organization has zero tolerance for Fraud and Corruption, which sets a strong tone from the top. This zero tolerance statement does not translate directly to the risk appetite and is often interpreted by stakeholders as 'zero tolerance for inaction' in the event of fraud. Although many agencies characterize themselves as 'highly risk averse', the concept of zero appetite is not considered practically sound and therefore a low risk appetite is referenced. Overall, there is some consistency across the system regarding the AFAC policy, however there exists opportunities to further harmonize and improve consistency of the policies within the UN system, Section 3.1 outlines a non-prescriptive list of some of the main components that organizations may choose to include in an AFAC policy and provides a brief overview of leading practice.

Although all respondents reported that their respective organizations follow the Institute of Internal Auditors' (IIA) Three Lines Model, there was notable inconsistency across the system regarding the custodian of the AFAC policy. It was noted that in 65% of organizations, the second line anti-fraud function was the custodian of the policy, whereas in the others, the responsibility ranged from the third line to the first line. There is emerging industry practice, particularly with the launch of the revised Three Lines Model, where the second line may be most suited as custodian, recognizing that practices and theories in this area differ.

3.1 AFAC Policy – Leading Practice

This section outlines a non-exhaustive list of key components typically included in an AFAC policy. It provides an overview of the content for each of these sections based on leading practices that have been selected as being the most practical and realistic to apply in an UN context. It also provides benchmarking across the UN system and other international organizations, which can then be tailored based on organizational requirements.

1. Scope

Leading practice: Should clearly outline stakeholders and activities that are subject to this policy. Such policies are applicable generally to all personnel, implementing partners, vendors and apply to all activities the organization engages in or funds to achieve its objectives.

2. Definitions

Leading practice: Policy clearly defines key terminology such as fraudulent; corrupt; collusive; coercive, and obstructive practices (see section 2.1). This will help ensure consistent usage and clear meaning throughout the policy. Some organizations may also reference money-laundering and terrorist financing within the definition.

3. Roles and Responsibilities

Leading practice: Policy clearly defines the roles and responsibilities of all internal stakeholders, including but not limited to: staff, non-staff, management/senior management and governing bodies (or equivalent). Furthermore, the policy should outline the divisions/units responsible for the management of fraud/corruption risk, the establishment and maintenance of the policy (including the custodianship of the policy) and the independent division/unit responsible for conducting the investigative activities and the level of management responsible for applying sanctions.

In addition, the roles and responsibilities of key external stakeholders should be clarified, for example, vendors and implementing partners. This should also include any expectation that the external stakeholders will conduct due diligence with their respective third parties.

4. Enterprise Risk Management (ERM)

Leading practice: Policy linkages to the organization's ERM framework should be highlighted in this section, including a clear indication of the organization's risk appetite and/or tolerance towards fraud and corruption (as applicable) (see section 7).

5. Prevention and Detection Measures

Leading practice: Policy outlines measures the organization has in place to help prevent/detect the occurrence of fraud. Such measures may include awareness training, due diligence, incorporating fraud prevention/detection into program design, fraud risk assessments, internal controls (delegation of authority, segregation of duties and accounting/reconciliations) and a fraud risk management function and culture (see section 4).

6. Reporting Fraud/Corruption

Leading practice: Reporting channels are clearly outlined in the policy. Generally, multiple confidential options are provided, further information in Section 8 – Reporting fraud. In order to encourage reporting, the policy should also clearly reference and/or indicate the organization's whistle-blower protection and/or protection from retaliation policy(ies) (see section 8).

7. Investigations

Leading practice: the policy should state the organizational unit responsible for conducting investigations. Generally, high-level principles are included in the policy, as opposed to procedures, which would be included in an internal procedural manual. The policy should also emphasize that the investigation is carried out confidentially. The level of confidentiality and promptness of the findings must be considered in order that the organization can learn from detected fraud to ensure systems weaknesses are addressed and trends monitored (see section 5).

8. Sanctions/debarment & Recoveries

Leading practice: the policy should clearly grant/delegate the authority to management (or designated official) to sanction persons/entities found to be involved in Fraud/Corruption following an official investigation. The policy should highlight the types of sanctions that may be applied when an investigation finds that a sanctionable practice has been substantiated. In addition, the policy should state the organization's options on recovering losses resulting from Fraud and Corruption. (see section 5).

9. Further considerations

As noted, the list is not exhaustive. Further considerations may include defined outcomes, review of established frauds for lessons learnt, identification of 'loopholes' and investigation of whether the same loopholes have been exploited elsewhere.

4. Prevention and Detection Measures

Fraud controls may be thought of as preventive or detective is nature. Preventive controls typically focus on encouraging the desired staff understanding and behavior in line with ethics expectations and most UN agencies align their code of conduct with their respective AFAC policy.

At the start of the Covid-19 pandemic, organizations were required to promptly adapt to a new reality, ranging from the shift to teleworking of its workforce to changes to their core procedures for their day-to-day activities and/or critical functions. Remote approaches to controls, especially for monitoring and due diligence, have been particularly important. Any change to the standard operating model can lead to increased risks of fraud and corruption, therefore organizations must continue to be vigilant and ensure that adequate mitigating controls are in place. Over half of the organizations have implemented special prevention measures or made amendments to their AFAC measures in light of the changes to operating contexts. Many organizations conducted an assessment of risks and controls in light of proposed changes during the pandemic, aiming to highlight residual risks arising from the changes. However, according to the survey, only half of UN Agencies require their third parties to conduct due-diligence or some form of assessment on their respective vendors/suppliers/recipients, which can result in an increased risk of fraud.

Adequate fraud prevention measures include key controls an organization can put in place to help mitigate the occurrence of fraud and corruption and support their early detection. Staff should have access to a handbook on prevention and detection of fraud and corruption (see below) or other comprehensive guidance, aligned to the organization's AFAC policy. The handbook can help internal stakeholders better understand how to prevent fraud and corruption in their day-to-day activities. Section 4.1 outlines some of the main components that should be included in a fraud prevention toolkit, providing a brief overview of leading practice.

4.1 Fraud Prevention Toolkit

1. AFAC Training Sessions for staff in High Risk Operations & during Emergencies

AFAC training sessions equip staff with knowledge and skills on fraud prevention, detection and risk management. The purpose of the training is to engage with colleagues who manage fraud risks in emergency contexts such as Covid-19, higher risk functions and operating environments with a view to building AFAC capacity.

Expected impact: Staff are empowered to address fraud and corruption risks and integrate AFAC practices into daily operational activities.

2. Training Kit on AFAC awareness for delivery by HQ and Field colleagues

Presentation material may be used by HQ and field colleagues to raise awareness with employees and third parties on the nature of fraud and corrupt practices, and their consequences. The kit can also clarify responsibilities for managing these risks, and share practical ways to prevent, detect, and respond to fraud.

Expected impact: Increased awareness and compliance with the AFAC policy.

3. Fraud Risk Assessment Guide

The Fraud Risk Assessment Guide provides practical guidance to managers and staff on conducting a fraud risk assessment. It builds on the principles, concepts and processes described in the Enterprise Risk Management policy and explains how these can be implemented in the context of fraud risks. It includes methods available to identify and assess fraud risks, such as, 'think-like-a-thief' and analyzing fraudulent acts at other organizations. It serves as a tool to help staff apply established risk and control mechanisms to manage the risk of fraud.

Expected impact:

- Promotes identification of potential vulnerabilities and enables the organization to become more resilient to fraud;
- Helps quantify exposures in terms of likelihood and impact and hence prioritize mitigating efforts;
- Acts as a strong fraud deterrent and a means to help managers allocate appropriate resources based on their assessment of the impact and likelihood;
- The causes and consequences of fraud can be better addressed when managers have regular and focused discussions on fraud related risks and hold parties accountable to apply existing controls effectively, identify control gaps and implement mitigation actions;
- Openness and transparency in relation to fraud risks will empower employees to come forward when they suspect that fraud may have occurred.

4. Handbook on Prevention and Detection of Fraud and Corruption

The handbook, available to all staff, should be developed with staff in the main functions of the organization and includes:

- Good practices in fraud prevention, mitigation, & lessons learned;
- Typical fraud schemes, warning signs and motivation for a minority to commit fraud;
- Prevention approaches: e.g. tone at the top, governance & oversight, fraud risk assessment, training & awareness, internal control implementation and monitoring;
- Detection approaches: e.g. identification of red flags, key risk indicators, data analytics, monitoring of business processes; unusual behavior;
- Ownership of the risk of fraud should be stated and based on 'Three Lines Model' (formerly the three lines of defense model);
- Internal controls for fraud risk management;
- Examples of actual fraud investigation cases in the organization.

Expected impact: The handbook aims to promote consistent fraud aware behavior and the development of stronger internal controls.

The handbook will assist in furthering the awareness of personnel and strengthening mitigating actions that will contribute to the prevention and detection of fraud and corruption within the organization as well as other parties working directly or indirectly through a partnership or other contract with the organization.

5. Catalogue of Fraud Risks in specific High Risk Functions

A catalogue of fraud risks in specific processes/ functions outlines fraud schemes and sample scenarios of fraud that could occur in those functions and should be mapped to the organization's risk categorization framework. It also includes mitigating controls for each scenario. It should be developed in consultation with the respective functions as a tool to help colleagues to identify and articulate potential fraud schemes during a fraud risk assessment and provide guidance on existing controls to mitigate the fraud schemes.

Expected impact: increased awareness of fraud & corruption risks in respective high- risk processes/ functions and risk mitigation actions.

6. AFAC Community of Practice social media platform

The AFAC Community of Practice (CoP) is an internal social media platform for all UN system staff to informally dialogue on issues related to fraud and corruption, share experiences, AFAC best practices and stay updated on corporate AFAC initiatives.

Expected impact:

- Promotes the growth of a strong AFAC culture to facilitate prompt reporting and the prevention and detection of fraud and corruption;
- Facilitates communication among personnel who work in high risk environments so that AFAC knowledge and good practices can be disseminated through the organization;
- Collects information on fraud and corruption risks to improve prevention and response;
- Stimulates interest in AFAC matters among colleagues worldwide.

Guidance material should be established for engagement in the CoP which respects the code of conduct, including confidentiality and privacy. There should also be guidelines on regular review and moderation of posts to the platform.

5. Fraud response and sanctions

It is essential that control gaps, in particular systemic issues, are addressed by management as soon as possible, and need not necessarily await case closure. This is a primary management accountability and should be conducted in consultation with second or third line input. Systemic issues may affect other activities or offices and therefore management should act promptly to ensure that any loopholes are closed, and thus losses minimized.

All fraud and corruption allegations received by organizations are reviewed to assess their credibility. All credible allegations are investigated by an independent investigation (or equivalent) function and generally conducted by internal staff with some outsourcing as needed. Once the investigation is complete, a summary of findings, conclusions, and recommendations are made to the decision-making body.

Findings concerning staff members are typically addressed through human resource related regulations and rules, and depending on the severity of the case, may result in a range of personal sanctions up to and including summary dismissal potentially with criminal proceedings.

Organizations typically establish a sanctions committee to review the findings, conclusions and recommendations stemming from the investigation of alleged fraud/corruption cases involving third parties. A sanctions committee may recommend to the appropriate authority sanctions including, but not limited to: letter of reprimand; contract termination; debarment; and conditional non-debarment. In addition, following an investigation and substantiation of an allegation of fraud or corruption, the majority of organizations estimate the financial impact and where possible, try to recover any losses. They may also invoke criminal proceedings.

In order to facilitate the implementation of sanctions, organizations are encouraged to implement clauses within legal agreements with all parties, noting their obligation to comply with the AFAC policy and clearly stating that the organization may impose sanctions or exit a contract in the case of non-compliance. UN Agencies should also request written confirmation from counterparties of compliance with AFAC policies and implement monitoring of such compliance, e.g. audits and fraud risk assessments.

Information on sanctions should be reported at summary level, ensuring confidentiality, to relevant governing bodies. In addition, an organization may report periodically to all personnel a summary of sanctions applied to staff and/or third parties in order to foster an anti-fraud, anti-corruption culture within the organization.

Systemic sharing of lessons and cases through relevant fora such as the Finance and Budget Network, Procurement Network and HR Network would greatly enhance fraud preparedness and prevention across the System. Furthermore, sharing information across UN agencies e.g. via the UN Ineligibility list, would be beneficial to protect other UN Agencies from engaging with counterparties debarred by one UN Agency.

6. Toolkits and training

Organizations have many toolkits and training courses in place to help promote fraud and corruption awareness, which include: operational guidance documents, awareness training for internal and external stakeholders, management specific training, information and communication regarding fraud reporting protocol, etc. The majority of organizations require mandatory fraud and corruption training for their staff and non-staff upon their appointment or contract start, with periodical updates.

The HLCM Cross-Functional Task Force on Risk Management has created a Risk Management Information Sharing platform and encourages all stakeholders to continue to share relevant tools and training on the platform.

Please refer to survey results, summarized in the Annex, which provide more details.

7. Assessing exposure to fraud and corruption

Most organizations conduct a periodic fraud and corruption risk assessment for ongoing activities, however, more importantly this also needs to be done for new activities and programs. These assessments, which may be conducted on a routine or ad-hoc basis, highlight control weaknesses that may lead to exposure to fraud and corruption. In turn, these fraud risks and/or control weaknesses may be recorded and monitored in the organization's Enterprise Risk Management system.

Please refer to survey results, summarized in the Annex, which provide more details.

8. Reporting fraud

Organizations have many mechanisms to promote and support the reporting of fraud and corruption, such as designated and confidential telephone numbers and emails, in-person reporting, etc. Reporting fraud is a primary responsibility of all staff and managers. All organizations who responded to the survey reported having sensitized staff and third parties about their whistle-blower protection programs, which aim to encourage fraud reporting. Over half of the organizations reported a significant increase of fraud and corruption over the past five years, many noting that this may be a result of increased awareness regarding fraud and corruption and the emphasis on protection against retaliation.

Please refer to survey results, summarized in the Annex, which provide more details.

Managing Fraud Risk

Annex – Anti-Fraud/Anti-Corruption Summary of Survey Results[3]

1. Organizations that participated in the survey

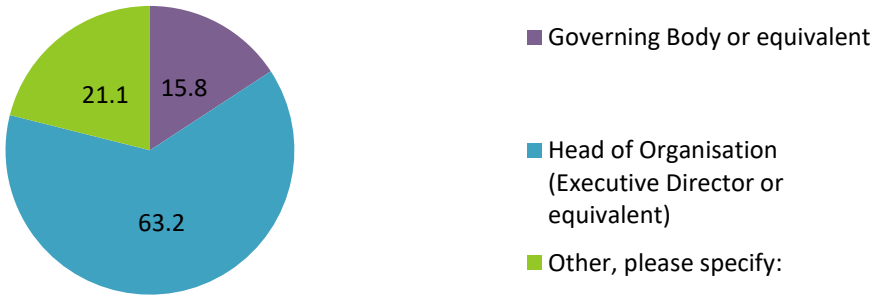
In April 2020, as part of the work of the Cross-Functional Task Force on Risk Management, the Managing Fraud Risk work stream administered a survey among the task force members. The following 18 organizations responded:

FAO	OECD	UNESCO	UNOPS
IAEA	UN Secretariat	UNFPA	WFP
ICAO	UN Women	UNHCR	WHO
IFAD	UNAIDS	UNICEF	WIPO
ILO	UNDP		

This Annex includes a summary of the findings. The survey garnered extensive individual comment from Organizations, which provides a rich source of information. A full set of anonymized results are available on the Risk Management Information Sharing platform.

2. Does your organization have an Anti-Fraud/Corruption Policy or similar (hereinafter, the 'Policy')?

3. If yes, please identify the final level of approval of this Policy?



[3] Note: a full version of results, with comments is available on the Risk Management Information Sharing platform

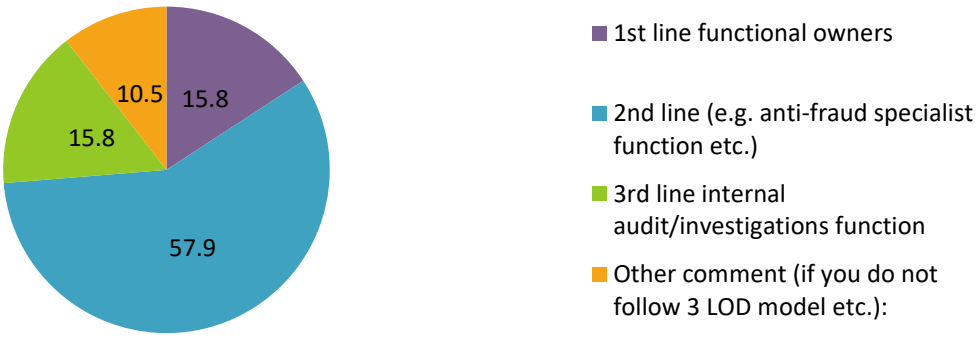
4. Does your organization have an anti-fraud strategy and action plan for

5. Does your organization follow the IIA's Three Lines of Defense Model?

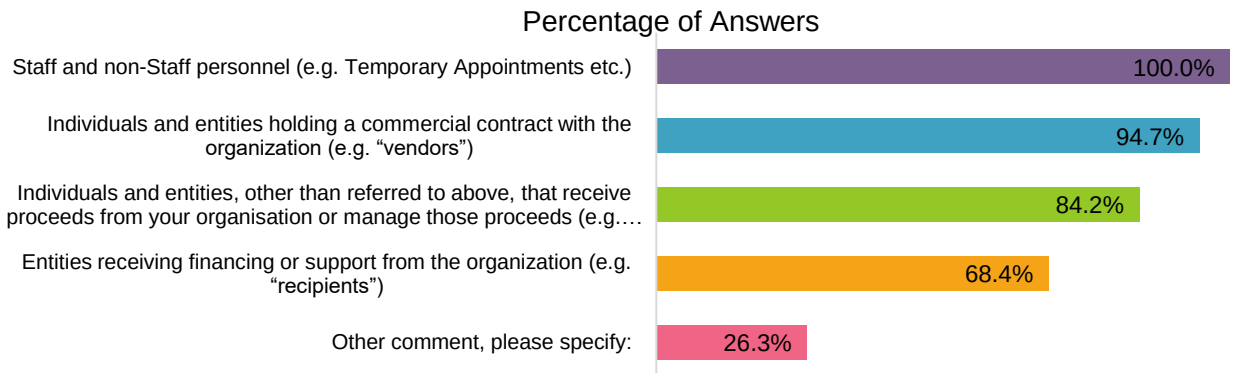
6. Does your AFAC Policy interrelate with your organization's ERM Policy/Framework? If yes, how?

[text responses]

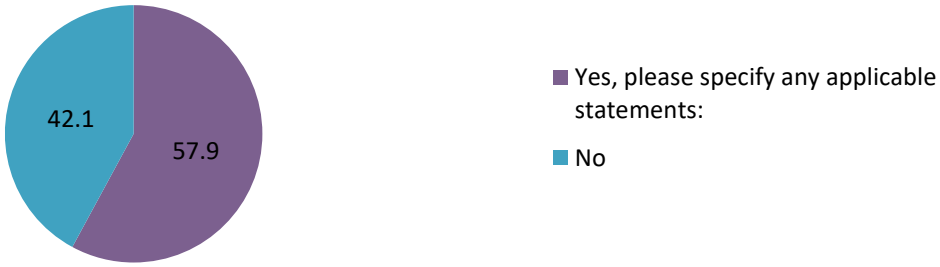
7. Within your organization, who is the custodian of the Policy?



8. What is the scope of the Policy? (select all applicable):



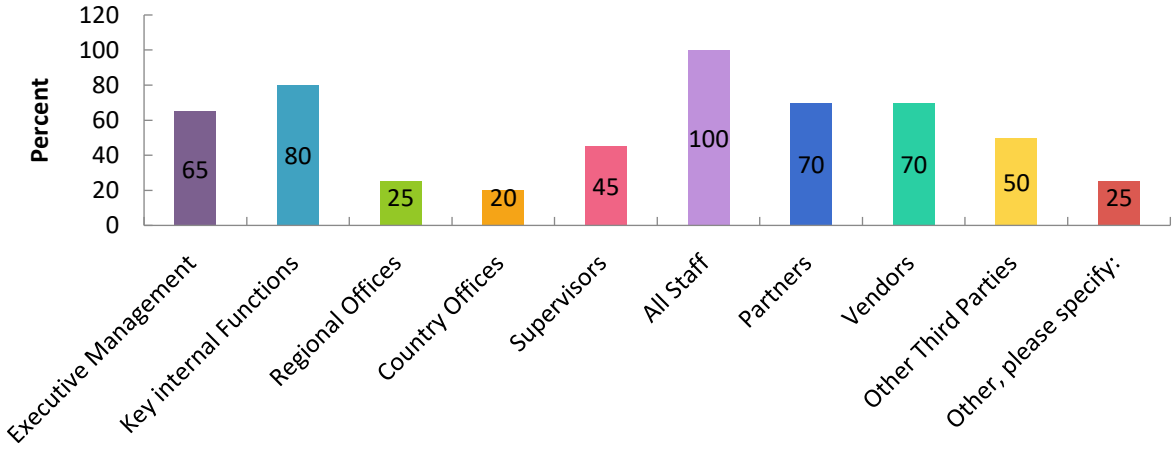
9. Does the Policy state a qualitative and/or quantitative risk Appetite or Tolerance level for Fraud/Corruption?



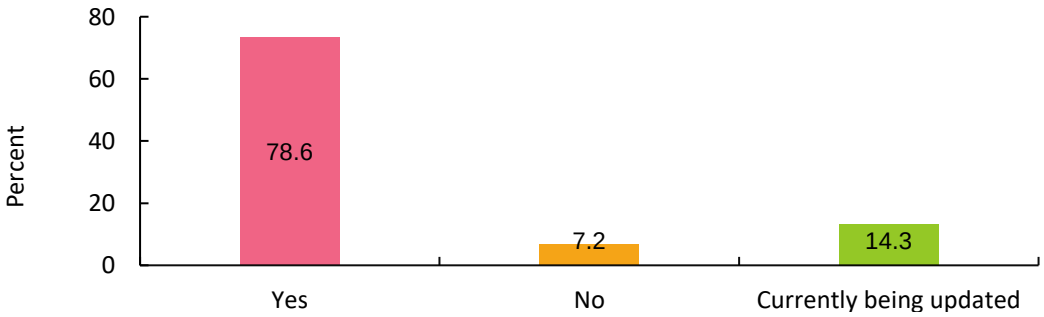
10. Would your organization consider adopting a common definition of anti-fraud/anti-corruption terminology (e.g. Fraud, Corruption, Prohibited Practices, etc.)?

- 81% of participants would consider adopting a common definition of anti-fraud/anti-corruption terminology.

11. The Policy outlines the responsibilities of (select all applicable answers):

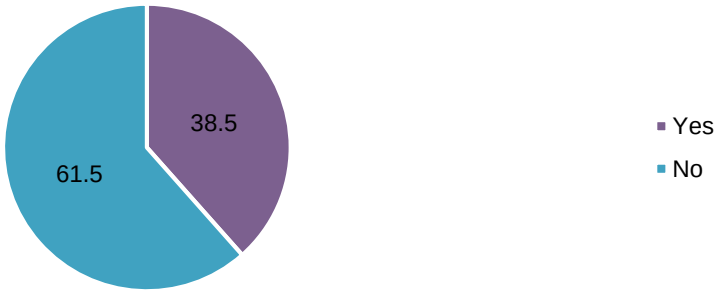


12. Your organization's Code of Conduct is aligned to the Anti-Fraud/Corruption Policy and shared with Staff, non-Staff and new recruits?



13. **Does your organization's Policy impose due diligence obligations on third parties vis-à-vis their contracts suppliers and stakeholders?**

14. **Is there a central repository for all fraud prevention/detection measures in place within the organization?**



15. **Does your organization have any insurance related for Fraud Risk? If so, please provide a brief overview of what it entails.**
[text responses]

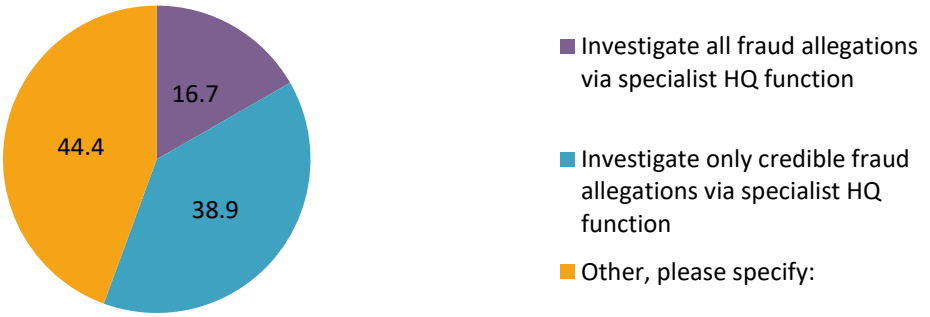
16. **In light of the current COVID-19 circumstances, has your organization implemented any special prevention measures or made amendments to its current measures related to Anti-Fraud/Anti-Corruption?***

17. **Has there been a review of risk/controls in the special measures due to COVID-19 noted in the question above and if so, how?**

[text responses]

18. **Does your AFAC Policy specifically cover fraud resulting from cybercrime? If so and in light of the current COVID19 circumstances, have additional controls been implemented to protect your organization from cybercrime?**
[text responses]

19. How does your organization respond to Fraud allegations?



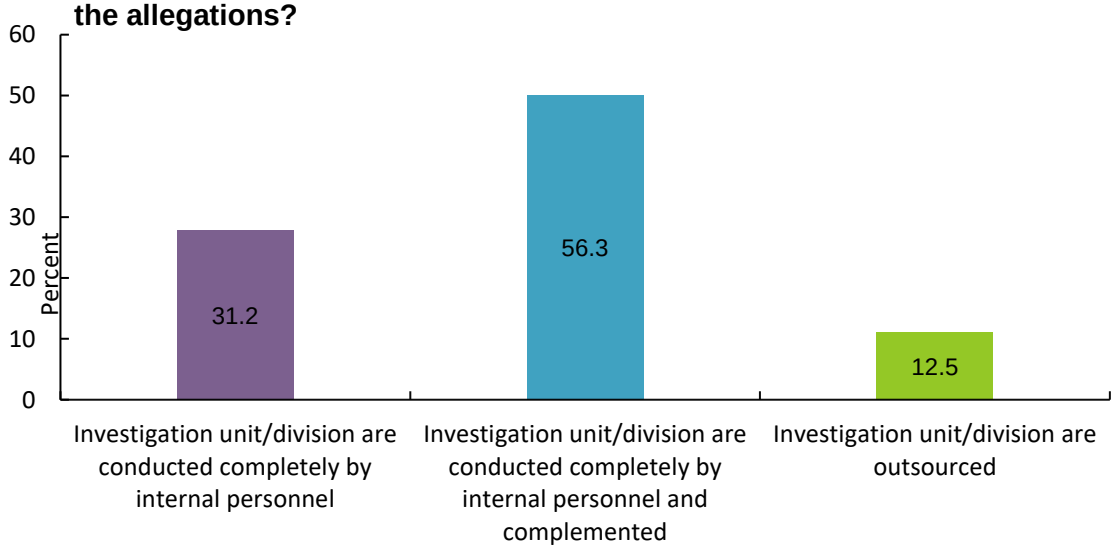
20. Which Unit/Division in your organization is mandated to investigate Fraud/Corruption Allegations?

[text responses]

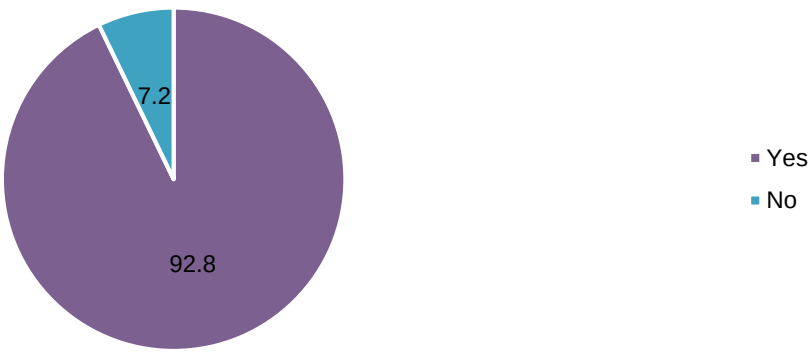
21. What is the Internal Audit function's role in the investigation process?

[text responses]

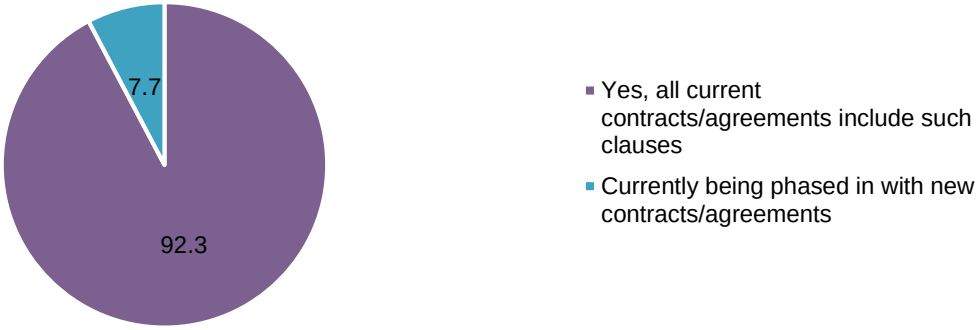
22. Please select the approach used by the responsible unit/division to investigate the allegations?



23. Does the Policy provide management the authority to sanction and/or terminate contracts with parties involved in Fraud/Corruption following an investigation?



24. Third party contracts highlight the requirements of adherence to the Anti-Fraud/Corruption Policy and provides the organization the authority to terminate the contract in case of breach?



25. Does your organization collaborate with other UN Agencies and/or local authorities during the investigation process?

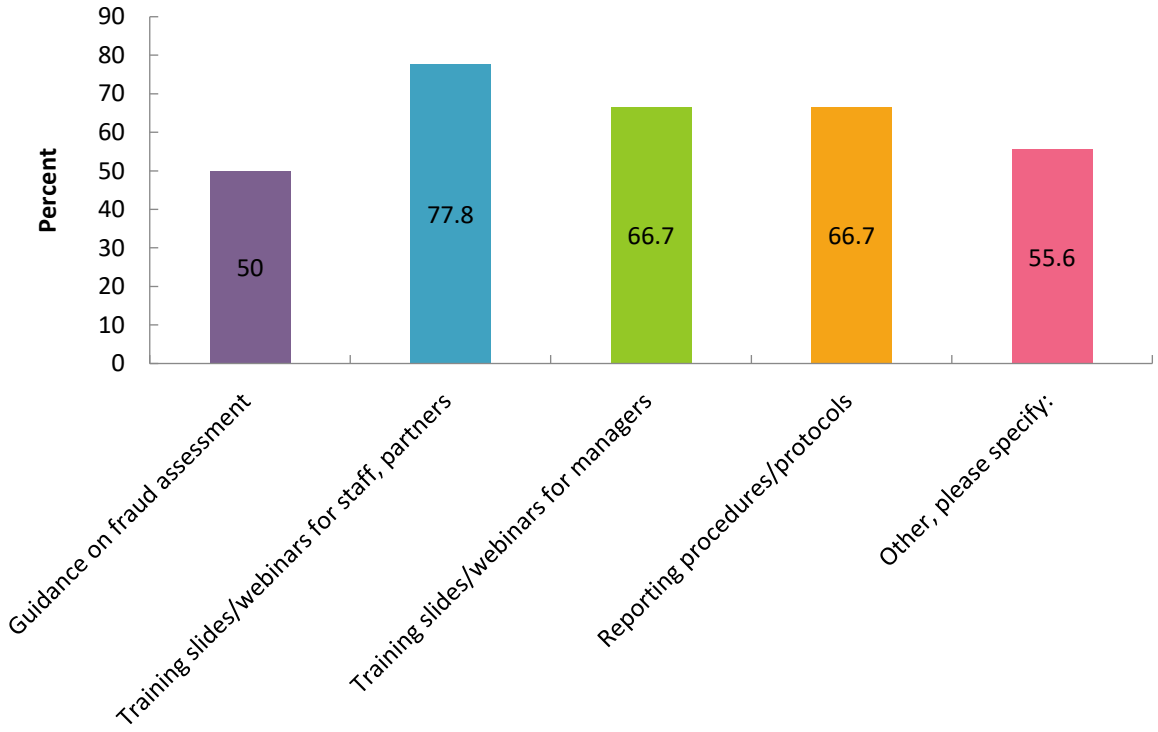
- **80% of participants** answered "Yes, where required". Please see comments below.

26. Does your organization share information on sanctions applied to staff and third parties?

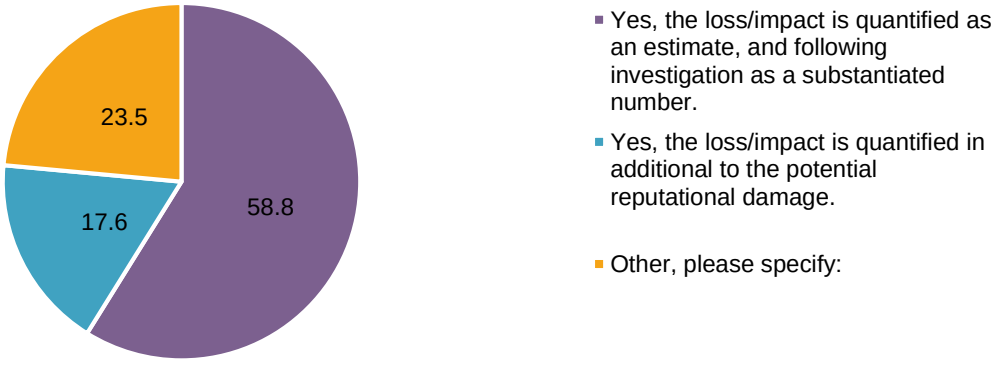
27. Does your organization use an IT Software solution for Fraud/Corruption Risk Management?

28. Does your organization require mandatory fraud prevention training course/programme for Staff and Non-Staff?*

29. Which tools (e.g. website, handouts, etc.) does your organization offer to support Staff, non-Staff and/or third parties to understand the Policy requirements and prevent and detect potential Fraud/Corruption in their day-to-day activities and interactions?



30. Once an alleged case of Fraud/Corruption is confirmed, does your organization estimates the impact of the case?



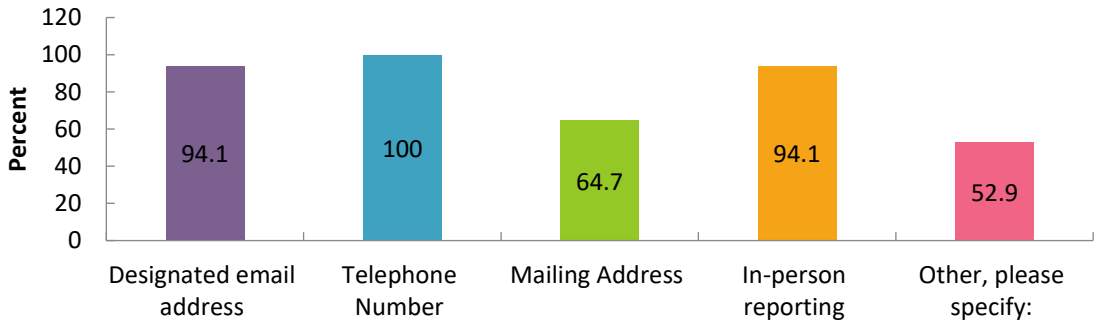
31. Does your organization pursue recovery of losses due to fraud/corruption and if so, which function is responsible for pursuing recovery?

[text responses]

32. Has your organization undertaken a Fraud Risk Assessment in the last 5 years? If so, please provide a brief overview of the scope of the review.

[text responses]

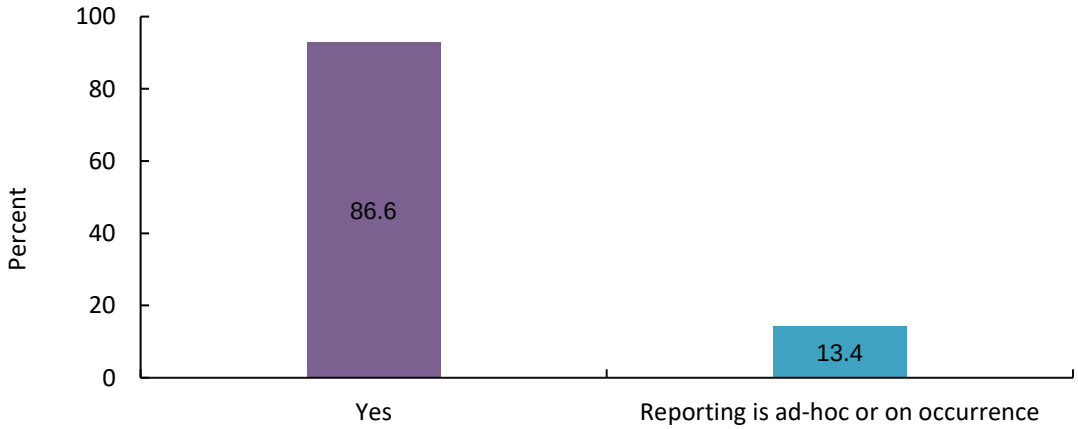
33. Select the options offered by your organization to report Fraud (Fraud Hotline).



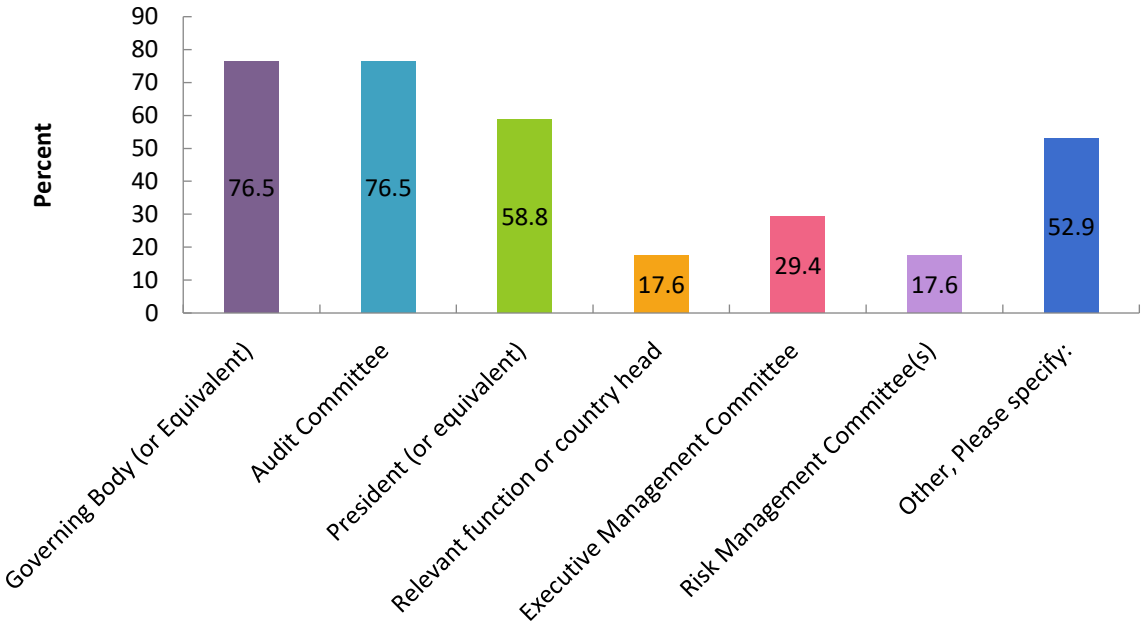
34. Does your organization have a whistle-blower protection mechanism, which is readily available to staff and the public?

All participants confirmed to have a whistle-blower protection mechanism available to staff and the public.

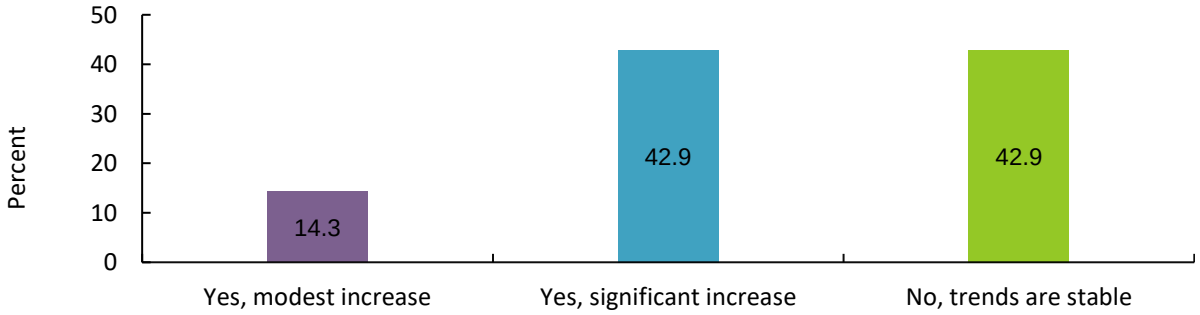
35. Does your organization prepare periodic reporting on the fraud cases identified, the outcome of the investigations and/or recoveries of fraud?



36. If yes, please identify recipients of the Fraud Reporting: (select all applicable)



37. Has there been an increase in Fraud/Corruption reporting over the few last years?



38. Any Additional Comments/Feedback

[text responses]