FRAUD rISK mANAGEMENT

Fraud Risk Assessment Guidance Note

**Introduction:**

In line with the United Nations’ zero tolerance to fraud and corruption, UNDP plays a significant role in the UN’s global effort to combat fraud and corruption, by supporting many countries in strengthening their capacity and framework to prevent fraud and corruption.

As stated in UNDP’s [Anti-Fraud Policy](https://popp.undp.org/_layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/AC_Internal%20Control%20Framework_Anti-Fraud%20Policy.docx&action=default), UNDP has zero tolerance towards fraud and corruption. UNDP staff members, non-staff personnel, vendors, implementing partners and responsible parties, irrespective of their nationality or background, must not engage in any forms of fraud. Fraudulent practices undermine UNDP’s efforts to promote social and economic development, which are core parts of UNDP’s mandate, and damage UNDP’s reputation. The intentional misuse or loss of resources violates our fiduciary responsibilities and will damage UNDP’s reputation which, in turn, will erode the confidence donor states have in the organization. This will lead to a reduction in or elimination of funding, which will jeopardize our ability to support our projects and maintain employment levels.

This guidance is developed to support UNDP personnel in preventing, detecting and responding to fraud and corruption. The primary purpose of this documents is to:

1. Strengthen fraud risk management including risk assessment and mitigating actions that will support in the detection and prevention of fraud against UNDP
2. Raise awareness of the various types of fraudulent acts, highlighting the most common fraud and corruption risks
3. Assist in promoting a culture of integrity by providing guidance on how to identify, manage and report fraud and corruption risks.

Fraud and corruption lead to significant financial risks, operational risks and most importantly, reputational risks. All these risks could jeopardize UNDP’s objectives and undermine its ability to fulfil its mandate.

All UNDP personnel have a significant role in the prevention, detection, reporting and mitigation of fraud. This includes the following:

1. Adhere to the Standards of Conduct for the International Civil Service, the code on conduct set in UNDP rules and regulations, policies and procedures and the provisions of contractual agreements;
2. Act at all times in accordance with the highest standards of integrity;
3. Under no circumstances, engage in, or facilitate, or appear to disregard or facilitate, any fraud and/or corruption in the course of the activities and operations of UNDP;
4. Refrain from participating in any activities that may cause any conflict of interest;
5. Avoid the misuse of funds, resources, and/or assets of UNDP
6. Detect, prevent and respond to any fraud and corruption, accordance with the Anti-Fraud Policy and strategy
7. Comply with the mandatory training requirements under the Anti-Fraud and Policy and Anti-fraud Strategy

**Fraud Risk Assessment**

Fraud Risk Assessment is part of the [Enterprise Risk Management (ERM) policy](https://popp.undp.org/SitePages/POPPSubject.aspx?SBJID=431&Menu=BusinessUnit)**.** The guide provides practical guidance on conducting a Fraud Risk Assessment which builds on the principles, and processes described in the ERM methodology and [UNDP ERM guide](https://info.undp.org/sites/ERM/Shared%20Documents/UNDP%20ERM%20Guide_Sept2019.pdf) and explains how these can be implemented in the context of fraud risks. It aims to help Country offices and Business Units to identify fraud risks and apply mitigation measures to manage them.

Fraud Risk Assessment can take place any time. However, there are particular occasions when a FRA is required as stated below:

1. Annually as part of offices’ risk assessments within the Integrated Annual Plan (IWP) exercise (IWP) process;
2. During regional bureau/functional oversight reviews of the Internal Control Framework (ICF) and internal controls
3. At the programme/project design stage;
4. Prior to or immediately following major changes in business processes;
5. Prior to major scale-up or scale-down of operations; and
6. Where there are sufficient concerns about the integrity of operations.

### 

Country Offices/Business Units must plan to conduct Fraud Risk Assessment at least once a year as part of the IWP exercise/Project design and development stage. Assessment outputs must feed into the general risk assessment process and be recorded in risk registers.[[1]](#endnote-1)**[[2]](#footnote-1)**

Fraud risk assessment should be conducted in a team and represents all key functions (procurement, finance, projects, etc..) that could result risk exposures. It should cover all key functional end to end business processes and thereafter at the office level. To ensure effective fraud risk assessment, relevant processes and procedures, documentations, and reports (e.g. Atlas Argus report), previous reports of fraud (including reports submitted to OAI and SECU), and observations from oversight missions, evaluations and audits must be reviewed and assessed. External sources of information such as recent media reports on fraud in other organizations, complaints from implementing partners and beneficiaries etc. could also provide useful insights on potential areas of fraud.

Based on the assessment, fraud risks should be identified, analyzed and prioritized along with mitigation measures to effectively manage the risks.

**Fraud Risk Identification:**

Possible risks to explore while identifying fraud risks include (but not limited) the following:

1. Procurement fraud and conflict of interest
2. Cash-for-work transfer fraud
3. Implementing partners fraud
4. Service provider fraud
5. Payment fraud
6. Misuse of resources
7. Travel fraud
8. Human Resources fraud
9. Assets fraud
10. Cyber fraud

Some possible causes of fraud risks:

1. Inadequate segregation of duties, delegation of authorities and Insufficient Internal Control Framework (ICF) for offices
2. Failure to take action on reported suspicions
3. Failure to identify conflicts of interest
4. Lack of coordination between UNDP and financial service provider to detect possible fraud issues
5. Inadequate monitoring and oversight
6. Failure to identify fraudulent activity following beneficiary complaints
7. Inadequate partners capacity assessment (partners did not have finance or human resource policies, and had poor financial management controls)
8. Partners don’t not maintain required records/supporting documentation
9. Failure to verify that service rendered prior to payment
10. Inadequate documentation checks prior to payment
11. Inadequate monitoring over UNDP assets
12. Inadequate ICT systems controls

Possible mitigation measures to mitigate those:

1. Clustering of services
2. Strengthening procurement process
3. Strengthening Vendor management process
4. Organizational controls: well-defined roles and responsibilities and strengthened monitoring and oversight
5. Segregation of duties and up to date ICF, for example, enhancing system controls to prevent initiation and completion of transactions by the same individual
6. Strengthening Implementing Partner (IPs) and Responsible Party (RP)selection and project implementation by adopting the Harmonized Approach to Cash Transfers (HACT) framework
7. Due diligence of personnel, partners and vendors.
8. Controls over payments
9. Trainings and certifications
10. Awareness raising and communication
11. Delegation of authority

**Risk Analysis (Likelihood and Impact)**

Considering existing measures and control activities, each risk should be assessed based on likelihood of occurrence and impact on objectives, on a 5-point scale as defined in the ERM Policy. the likelihood and impact of each risk should be objectively scored, considering data that may support the scoring including previous fraud cases or losses that are relevant for the office or functional area; relevant indicators or red flags that may suggest weak controls or unusual events; and relevant oversight/OAI findings.

When assessing likelihood , consider future probability or the frequency of occurrence in the past as described in the ERM policy scale below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood | Not likely | Low likelihood | Moderately likely | Highly likely | Expected |
| **1** | **2** | **3** | **4** | **5** |
| Description  (“The risk is expected to materialize….”) | Every 5 years or less  **and/or**  very low chance (<20%) of materializing | Every 3-5 years  **and/or**  low chance (20% - 40%) of materializing | Every 1-3 years  **and/or**  chance of materializing between 40% - 60% | Once or twice a year  **and/or**  high chance of materializing (60% - 80%) | Several times a year  **and/or**  chance of materializing above 80% |

The impact scale considers financial, reputational, compliant consequences that UNDP could encounter when fraud occurs including the impact on UNDP’s development results and operations as described below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Impact | | Negligible | Minor | Intermediate | Extensive | Extreme |
| **1** | **2** | **3** | **4** | **5** |
| Description of consequence | **Financial**  **(absolute and relative)** | Estimated range in USD, 3 numbers:   * Maximum (highest level of potential deviation, +/-)) * Likely (*best guess*) * Minimum (*lowest level of potential deviation, +/-)* )   which, based on best guess figure, corresponds to: | | | | |
| <5 % deviation from applicable budget | 5-20 % deviation from applicable budget | 20-30% deviation from applicable budget | 30-50% deviation from applicable budget | >50% deviation from applicable budget |
| **Development results** | Negligible/no impact on results/outcome, positive or negative | 5-20 % of the applicable and planned results/outcome affected, positively or negatively | 20-30% of the applicable and planned results/outcome affected, positively or negatively | 30-50% of the applicable and planned results/outcome affected, positively or negatively | More than 5O% of the applicable and planned results/outcome affected, positively or negatively |
| **Operations** | Delay or acceleration of applicable operations by 1-2 days | Delay or acceleration of applicable operations 2-7 days | Delay or acceleration of applicable operations 1-4 weeks | Delay or acceleration of applicable operations for one month or longer | Permanent shift in applicable operations |
| **Compliance** | Negligible deviation from applicable rules and regulations | Moderate deviation from applicable rules and regulations | Deviation from applicable rules and regulations | Significant deviation from applicable rules and regulations | Major deviation from applicable rules and regulations |
| **Safety & Security** | No Effect on UNDP Personnel,  and/or  No effect on UNDP Operations and programmes | Slightly Injurious Effect on UNDP Personnel  and/or  injuries to general population directly or indirectly caused by UNDP actions | Moderately Injurious or Psychologically Traumatic Effect and/or  major injuries to general population directly or indirectly caused by UNDP actions | Fatal (individual or small numbers), Severely Injurious or Severely Psychologically Traumatic Effect  and/or  loss of life to general population directly or indirectly caused by UNDP actions | Catastrophically Fatal Effect (mass casualties)  and/or  loss of life to general population directly or indirectly caused by UNDP actions |
| **Reputation** | Isolated negative or positive comments from external stakeholders | Several negative or positive comments from external stakeholders | Negative or positive reports/articles in national, regional  and/or international media | Negative or positive reports/articles in several national, regional  and/or international media for a period of a week or more, and/or criticism from key stakeholders | Negative or positive reports/articles in several national, regional  and/or international media for a period of a month or more, and/or strong criticism from key stakeholders |

A risk may have a major impact when it occurs, but the likelihood of it happening is minimal. On the other hand, a risk with a minor impact may turn into a major risk for the organization if it occurs frequently. Therefore, it is important to monitor risks and changes in risks’ significance (likelihood X impact) using the ERM Dashboards’ risk heat map: [Project Risk Dashboard](https://app.powerbi.com/groups/34e1e0b6-b985-40f3-8351-1bad930325a2/reports/94f16fc4-4ec4-43cc-812c-19a03a6f91c3/ReportSection6b3809d26e1656f8eaf6?noSignUpCheck=1) and [Programme Risk Dashboard](https://app.powerbi.com/groups/34e1e0b6-b985-40f3-8351-1bad930325a2/reports/3c724978-c309-4815-84f1-89d31df22343/ReportSection5?ctid=b3e5db5e-2944-4837-99f5-7488ace54319).

Depending on the analysis, high significance risks require additional thorough assessment, HQ subject matter experts may be contacted to support in the additional review of the high-risks identified. It is important to well-document the review process the mitigation measures that are put in place to manage these high risks. In some cases, however, circumstances pertaining to the treatment itself may exceed the authority/mandate of the Risk Owner. Risk should be escalated if the Head of Office/Risk Owner considers that the risk meets one or more of the ERM policy [escalation criteria](https://info.undp.org/sites/ERM/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/ERM/Shared%20Documents/Risk%20Escalation%20Guidance.docx&action=default).

### Fraud risk monitoring, review, recording and reporting follows UNDP’s ERM methodology. For further information about ERM methodology, please refer to the [ERM policy](https://popp.undp.org/SitePages/POPPSubject.aspx?SBJID=431&Menu=BusinessUnit) and [ERM guide](https://info.undp.org/sites/ERM/Shared%20Documents/UNDP%20ERM%20Guide_Sept2019.pdf).

**Reporting fraud**

Effective Fraud Risk Management requires reporting or sharing any information about fraud or other corrupt practices against UNDP or involving UNDP staff, non-staff personnel, vendors, implementing partners and responsible parties, as indicated in the [Anti-Fraud Policy](https://popp.undp.org/_layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/AC_Internal%20Control%20Framework_Anti-Fraud%20Policy.docx&action=default).

Below are various channels to report allegations of fraud and corruption practices:

1. By email to OAI at [reportmisconduct@undp.org](mailto:reportmisconduct@undp.org) or directly to the Director, Office of Audit and Investigations, or Deputy Director, Head of Investigations, Office of Audit and Investigations**.**
2. Through an [online form](https://secure.ethicspoint.eu/domain/media/en/gui/104807/lang.html) accessible through the “Report fraud, abuse and misconduct**”**
3. Through an independent telephone service:
   1. Worldwide numbers are accessible through the “Report fraud, abuse and misconduct” [link](https://secure.ethicspoint.eu/domain/media/en/gui/104807/phone.html) (with interpreters available 24 hours/day)
   2. In the United States: 1-844-595-5206
4. By mail addressed to: Director, Office of Audit and Investigation, or Deputy Director, Head of Investigations, Office of Audit and Investigations, One United Nations Plaza, DC1, 4th Floor, New York, NY 10017, USA.

1. [↑](#endnote-ref-1)
2. Atlas for Project Risks and Corporate Planning System (CPS) for Programme risks [↑](#footnote-ref-1)