Risk management tool
FRAUD PREVENTION
<table>
<thead>
<tr>
<th>Title</th>
<th>Slide No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background and Purpose / Resource links / How to use the tool?</td>
<td>3</td>
</tr>
<tr>
<td>Risk Event</td>
<td></td>
</tr>
<tr>
<td>• Fraud in registration and targeting</td>
<td>4</td>
</tr>
<tr>
<td>• Fraud in UNHCR Mandate Refugee Status Determination (RSD) / Case processing</td>
<td>5</td>
</tr>
<tr>
<td>• Fraud in resettlement</td>
<td>6</td>
</tr>
<tr>
<td>• Fraud committed by Persons of Concern (PoCs)</td>
<td>7</td>
</tr>
<tr>
<td>• Fraud and corruption in the procurement process</td>
<td>8</td>
</tr>
<tr>
<td>• Instances of fraud and corruption by UNHCR funded partners (incl. government entities, partner personnel and sub-contractors)</td>
<td>9</td>
</tr>
<tr>
<td>• Fraud linked to undue influence on UNHCR processes by government authorities, donor countries and other entities</td>
<td>10</td>
</tr>
<tr>
<td>• Fraud in distribution and services to PoCs, including Cash Based Interventions (CBI)</td>
<td>11</td>
</tr>
<tr>
<td>• Diversion of aid (financial resources, inventory, non-food items and other assets)</td>
<td>12</td>
</tr>
<tr>
<td>• Fraud in recruitment processes and career progression</td>
<td>13</td>
</tr>
<tr>
<td>• Fraud in personnel benefits and entitlements, including the submission of Medical Insurance Plan claims and in leave and absence management</td>
<td>14</td>
</tr>
<tr>
<td>• Fraud in personnel management related to travel, training and missions</td>
<td>15</td>
</tr>
<tr>
<td>• Fraud linked to the use of UNHCR’s assets, inventories and supplies</td>
<td>16</td>
</tr>
<tr>
<td>• ICT, Cyber and Data Fraud</td>
<td>17</td>
</tr>
<tr>
<td>Opportunity</td>
<td></td>
</tr>
<tr>
<td>• Success in collaboration to combat fraud with stakeholders involved in the PoC response</td>
<td>18</td>
</tr>
</tbody>
</table>
BACKGROUND AND PURPOSE

An effective fraud prevention, detection and response capacity is vital for UNHCR’s ability to discharge its mandate effectively and credibly for refugees and other persons of concern (PoCs). Fraud risk management is also a crucial part of good governance and therefore helps safeguard UNHCR’s reputation.

The 2013 UNHCR Strategic Framework for the Prevention of Fraud and Corruption provides the definition of fraud and corruption, as well as a detailed outline of UNHCR’s policy and methods related to the prevention of and response to fraud.

Fraud in UNHCR is defined 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” (see Handbook on Fraud and Corruption Prevention, Detection and Reporting at UNHCR).

The Enterprise Risk Management Service (ERM) has developed this tool which the aim to assist field operations to better understand and manage fraud risks across a wide range of UNHCR’s activities. The tool is designed to help ensure that key risks have been adequately identified and analysed, and that relevant treatments - proactive and reactive - have been considered thoroughly and agreed upon within the operation.

It is important to keep in mind that the risk management process may also facilitate the identification of new opportunities, thereby enhancing the possibilities of achieving objectives for the operation.

The tool is purely an advisory resource; the authority to issue mandatory instructions for mitigating fraud risks rests with the respective entities, for instance, DFAM for financial management and DIP for fraud committed by persons of concern. The IGO has the sole authority to initiate investigations. UNHCR personnel should report suspected fraud to the IGO without delay, i.e. via e-mail: inspector@unhcr.org.

The tool comprises of several key risks, with examples of causes, consequences and treatments that may apply in your operation. These risks and treatments are the result of an analysis of the operational risk register, relevant sectoral policies and guidelines, and field colleagues’ contributions.

While the tool attempts to be as exhaustive as possible, there may still be elements of risks and treatments that have not been captured. Operations are welcome to contribute by sending additional proposals and comments to hqerm@unhcr.org, with subject: Tool - Fraud Risks.

Since this tool is covering fraud in a wide range of UNHCR’s activities it is recommended to consult the resources listed below.

HOW TO USE THE TOOL?

Operations can select one or more risk event(s) that apply to their operation, as well as the applicable causes, consequences and treatments. Please note that none of the Proactive or Reactive treatment “menu” is compartmentalised; treatments can be applicable to one or several causes or consequences. All statements (cause, event, consequence and treatments) can be edited and adjusted to your operational context; some may not be relevant or possible in each context. Key risks should also be reflected in the operation’s overall online risk register. If multiple risks from the tool are relevant to your operation, we would suggest capturing them in one or two higher level risks to keep the overall risk register as a streamlined, prioritised management tool for the Representative and senior management team. Please ensure to select the tag “Fraud”. Some fraud risk events are covered in greater details in the other risk management tools e.g. Implementing with Partners, Resettlement and Complementary Pathways, Procurement. Visit the ERM Risk Management Toolkit intranet page.

RESOURCE LINKS

UNHCR Strategic Framework for the Prevention of Fraud and Corruption (2013)
Handbook on Fraud and Corruption Prevention, Detection and Reporting at UNHCR (2017)
Policy on Addressing Fraud Committed by Persons of Concern, HCP/2017/3/Rev.1
Operational Guidance on Addressing Fraud Committed by PoCs, UNHCR/OG/2017/1/Rev.1
UNHCR Resettlement Handbook (July 2011 Edition)
Key policies and guidance on enterprise risk management (ERM Service Intranet site)
E-learning - Prevention of Procurement Fraud (unhcr.org)
E-learning - Fundamental of Fraud and Corruption Awareness

“A risk statement as reflected in the online Risk Management Tool consists of four parts, namely, a risk event, its causes, consequences and a name. A risk may have multiple causes and consequences but has only one risk event. The risk name should be succinct and clearly identify the risk. Risk treatments are actions to reduce the likelihood and impact of the risk. Proactive risk treatment actions are implemented before a risk event occurs, based on identified causes of the risk event. Reactive risk treatments are executed after a risk event occurs, thus addressing the consequences of the risk event occurring.”
## Risk event | Fraud in registration and targeting

<table>
<thead>
<tr>
<th>Causes</th>
<th>Proactive treatments</th>
<th>Consequences</th>
<th>Reactive treatments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenging environment, e.g. emergency, or prevalence of fraud in the operating context</td>
<td>Raise awareness among PoCs and increase effective visibility of consequences of fraud/corruption</td>
<td>Diversion of funds as those not qualifying receive assistance</td>
<td>Review and remedy the cause of the established fraud</td>
</tr>
<tr>
<td>Adequate anti-fraud procedures and associated checks and balances are not in place for individual case processing, including review of registration and Refugee Status Determination (RSD) and resettlement decisions by senior management</td>
<td>Engage in inter-agency and multi-functional needs assessments</td>
<td>Aid not reaching PoCs targeted by the relevant assistance activities</td>
<td>Revise the targeting criteria</td>
</tr>
<tr>
<td>Lack of monitoring, including of measures put in place in response to identified shortcomings</td>
<td>Plan for a proper vulnerability assessment, using relevant guidelines and seeking expert support, and as relevant, coordinate with other agencies and partners to ensure consistency</td>
<td>Unreliable data leading to incorrect planning, budgeting and reporting</td>
<td>Recover amounts unduly paid</td>
</tr>
<tr>
<td>Insufficient internal controls allowing personnel to manipulate registration data for personal gain</td>
<td>Ensure targeting criteria are clear, specific, verifiable, communicated to PoCs and aligned with the assessments, policies and programmatic objectives</td>
<td>Damage to UNHCR’s organizational reputation and negative effects on the integrity of the registration, RSD, and resettlement processes</td>
<td>Report suspected cases of fraud to the Inspector General’s Office (IGO)</td>
</tr>
<tr>
<td>Unclear guidance on how to implement targeting exercise</td>
<td>Run statistical analyses to detect for example unusual high or repeated payments</td>
<td>Loss of donor, inter-agency and partner confidence regarding the reliability of UNHCR registration data</td>
<td>Engage with communities, communicate remedial action to communities, document safeguards put in place and reinforce monitoring</td>
</tr>
<tr>
<td>Non-segregation of duties related to targeting and distribution</td>
<td>Ensure complaint mechanisms are in place and raise awareness of beneficiaries of their rights to use complaint hotline (if established) and other outreach mechanisms</td>
<td></td>
<td>Inform host government authorities about established fraud</td>
</tr>
<tr>
<td>Falsified information provided by PoCs</td>
<td>Conduct Post Distribution Monitoring (PDM), contact beneficiaries to confirm the receipt of cash, goods or services distribution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insufficient documentation/data of PoCs</td>
<td>Ensure effective use and monitoring of anti-fraud controls in the proGres database and BIMS biometric system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNHCR’s and partners’ limited personnel capacity (numbers, knowledge)</td>
<td>Conduct surveys and interviews to assess accuracy and effectiveness of the targeting criteria ensuring Age Gender Diversity (AGD) approach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability by other parties to inflate population data, redirect services or otherwise influence the targeting and registration process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corrupt or compromised targeting criteria (receipt of bribes, extortion or coercion) or list</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk event</td>
<td>Fraud in UNHCR Mandate Refugee Status Determination (RSD) / Case Processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Causes</strong></td>
<td><strong>Proactive treatments</strong></td>
<td><strong>Consequences</strong></td>
<td><strong>Reactive treatments</strong></td>
</tr>
<tr>
<td>Issuance of UNHCR documents and registration, RSD and resettlement systems and processes do not have sufficient anti-fraud controls</td>
<td>Duly implement <em>Procedural Standards for Refugee Status Determination under UNHCR’s Mandate</em></td>
<td>Diminished protection space</td>
<td>Review and remedy the cause of the established fraud</td>
</tr>
<tr>
<td></td>
<td>Ensure the deployment / availability of biometrics as a matter of priority</td>
<td>Individuals not in need or not deserving international refugee protection receive refugee status</td>
<td>Ensure referral to anti-fraud focal point and panel as per SOPs</td>
</tr>
<tr>
<td></td>
<td>Strengthen complaint and feedback mechanisms and raise awareness with personnel / PoCs / communities with regard to fraud</td>
<td>Loss of integrity of UNHCR processes including resettlement, UNHCR’s assistance going to undeserving persons not in need or not deserving international refugee protection</td>
<td>Reassess and strengthen if required RSD process and training needs</td>
</tr>
<tr>
<td>Lack of or insufficient management oversight in the RSD process</td>
<td>Ensure relevant personnel is adequately trained and supervised in line with the RSD Procedural Standards</td>
<td>Loss of organizational credibility and reputation</td>
<td>Refer suspected misconduct by personnel / partners to IGO</td>
</tr>
<tr>
<td>Non-availability of biometrics</td>
<td>Request the deployment of additional, trained RSD personnel for example through a deployment scheme.</td>
<td>Loss of donors’ confidence and support to RSD and/or resettlement programmes</td>
<td></td>
</tr>
<tr>
<td>Lack of fraud awareness among personnel involved in registration and RSD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limited personnel capacity (numbers, knowledge) or high turnover of personnel</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Risk management tool: Fraud Prevention**
## Risk event | Fraud in resettlement

### Causes
- Discrepancy between demand of resettlement places and their availability
- Inexistent or inadequate mechanisms to identify and report fraud
- Persons of concern are not given adequate information about the resettlement process / process leading to complementary pathways and/or regular updates about the status of their case
- Insufficient case processing oversight and monitoring
- Failure or delay in responding to fraud allegations
- SOPs are not formally adopted, followed or updated
- Identification and referral mechanisms are procedurally weak or not in place
- UNHCR and/or partner personnel are able to engage in exploitation of refugees and/or other forms of misconduct

### Proactive treatments
- Designate anti-fraud focal point and ensure that he/she is leading the implementation of relevant policy and operational guidelines
- Provide anti-fraud training for personnel, partners and governments
- Conduct regular reviews, audits and random spot-checks of case processing and case management
- Ensure development of SOPs as well as awareness raising and training of staff on them
- Share information and provide counselling to individuals and communities to manage expectations
- Ensure availability and sharing of anti-fraud information material in relevant languages with individuals and communities, including on feedback and complaint mechanisms
- Include PoCs in anti-fraud initiatives
- Implement/enhance regular fraud reporting mechanisms and trends monitoring
- Ensure timely resolution of identified fraud cases in line with [Policy on Addressing Fraud Committed by Persons of Concern](https://www.unhcr.org/60e2b2d68.html) and its updated [Operational guidelines (OG)](https://www.unhcr.org/60e2b2d68.html)
- Request DIP Multi-Functional Integrity support missions to assess the integrity of protection systems and processes
- Share clear messages on possible consequences of fraud to PoCs
- Maintain effective feedback and complaint mechanisms tailored to the needs and capacities of persons of concern; ensure Prevention of Sexual Exploitation and Abuse mechanisms in place ([SEA risk tool](https://www.unhcr.org/60e2b2d68.html))

### Consequences
- Reduced resettlement and complementary pathways opportunities or programme put on hold
- Refugees in need of resettlement as a lifesaving, protection solution cannot access resettlement
- PoCs lose trust in UNHCR
- Security of PoCs or personnel at risk
- Public and political support for resettlement and complementary pathways declines
- Governments demand extensive implementation of remedial measures
- Governments turn to other partners to deliver resettlement services
- Reputational damage and loss of credibility for UNHCR
- Personnel motivation and work morale is diminished

### Reactive treatments
- Organize through the Bureau, Integrity Unit and/or Resettlement and Complementary Pathways Service a coordinated briefing for resettlement states, donor community and other stakeholders on allegations/instances of fraud (no-surprise approach)
- Issue public statements or response in coordination with the regional bureau and/or Resettlement and Complementary Pathways Service
- Decide on temporary suspension of resettlement programming in concerned operation(s) to address integrity gaps
- Initiate DIP Multi-Functional Integrity support missions to assess the integrity of protection systems and processes
- Initiate IGO and/or local investigation
- Provide stakeholders with periodic updates on fraud allegations and investigations (also a proactive treatment)
- Establish protocol for informing resettlement counterparts when allegations or incidents of fraud/corruption are committed by personnel or partners (also a proactive treatment)
## Risk event | Fraud committed by Persons of Concern (PoCs)

<table>
<thead>
<tr>
<th>Causes</th>
<th>Proactive treatments</th>
<th>Consequences</th>
<th>Reactive treatments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dire (or deterioration of) living conditions and financial situation of PoCs</td>
<td>Ensure thorough and meaningful review of registration, RSD and resettlement (SOPs) to maintain quality and integrity</td>
<td>Diversion of funds as those not qualifying receive assistance or large-scale sale of assistance items</td>
<td>Delay resettlement processing of implicated individuals</td>
</tr>
<tr>
<td>Insufficient documentation and data on PoCs</td>
<td>Appoint and train the Anti-Fraud Focal Point and ensure the implementation of relevant policy and operational guidelines, beginning with fraud vulnerability assessment</td>
<td>Undermined protection processes and assistance</td>
<td>Request DIP Multi-Functional Integrity support missions to assess the integrity of protection systems and processes (also a proactive treatment)</td>
</tr>
<tr>
<td>Failure to implement registration and screening process according to UNHCR policy and guidelines</td>
<td>Establish a Fraud Assessment Panel and ensure effective oversight and management of the cases</td>
<td>Damage to UNHCR’s reputation and negative effects on the integrity of the registration, RSD and resettlement processes</td>
<td>Temporarily suspend resettlement programming in concerned operation(s) to address integrity gaps</td>
</tr>
<tr>
<td>PoCs have access to and use false documents and/or identity to access UNHCR protection and services</td>
<td>Outline key protection, assistance and solutions interventions to PoCs and develop relevant SOPs</td>
<td>Loss of donors’ trust and possibly funding</td>
<td>Prepare a crisis communication with donors e.g., holding statement, Q&amp;A</td>
</tr>
<tr>
<td>Inadequate internal controls for fraud prevention. SOPs in regard to protection and assistance delivery not adhered to</td>
<td>Plan for and conduct a proper PoC vulnerability assessment, using relevant guidelines and seeking expert support</td>
<td>Security of PoCs may be at risk</td>
<td>Escalate to the regional bureau or HQs entity</td>
</tr>
<tr>
<td>Cuts in assistance and reduced availability in resettlement quotas</td>
<td>Implement biometrics. Ensure effective use and monitoring of anti-fraud controls in the proGres database and BIMS biometric system</td>
<td></td>
<td>Collaborate with Government or local authorities in case of referrals to national justice systems</td>
</tr>
<tr>
<td>Personnel not trained or aware of typical fraud schemes</td>
<td>Conduct anti-fraud training to personnel and partners</td>
<td></td>
<td>Consider in consultation with LAS and the Bureau other recourses such as national justice systems to protect UNHCR’s interest and recover UNHCR funds</td>
</tr>
<tr>
<td>Monitoring failure or delay in responding to fraud allegations</td>
<td>Ensure monitoring and oversight on delivery of services and distribution to PoCs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Raise awareness among PoCs and increase effective visibility regarding fraud/corruption and the consequences</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disseminate key messages, such as UNHCR services are free, how to lodge a complaint, how to access services, duty of personnel, handling of confidential information, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure complaint mechanisms and outreach are in place and raise awareness of PoCs of their rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organize counselling to PoCs on registration and RSD procedures including complaint mechanisms</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inform PoCs about UNHCR safeguards to ensure fair protection processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Involve – where appropriate -government authorities (IDPs) in preventing fraud by PoCs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk event</td>
<td>Fraud and corruption in the procurement process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Causes** | Lack of segregation of duties in the procurement process  
Lack of internal controls, lack of oversight in the procurement process  
Suppliers unaware of UNHCR’s purchasing and procurement process  
Bribery or extortion by supplier to corrupt UNHCR personnel to influence, secure or extend a procurement contract  
Suppliers collude or “rig bids” to fraudulently secure procurement contracts, e.g. via a cartel  
Supplier fraudulently misrepresents its capacity to supply what is requested by UNHCR  
Supplier or another third party fraudulently submits false or incorrect invoices  
Supplier tables change order requests after a contract is awarded that are unjustified. This is a particular risk with construction contracts  
Weak control over establishment or change in supplier bank details  
Deterioration of local economy may increase fraud prevalence in order to make ends meet  
There is an external environment of fraud and corruption  
UNHCR personnel not aware of proper procurement procedures  
Personnel does not disclose conflict of interest with supplier and is engaged in a procurement process affecting that supplier  
Personnel accepts a bribe or gift or is otherwise coerced by a supplier to influence a procurement process |
| **Proactive treatments** | Hold supplier seminars on “How to do business with UN / UNHCR”  
Suppliers agree to UN Code of Conduct for suppliers and include it in the contract  
Ensure that all personnel are aware of who, how and when they can contact suppliers  
Ensure relevant personnel follow the online training: Prevention of Fraud in Procurement  
Review for signs of collusion or bid rigging in supplier responses and perform due diligence checks on suppliers  
Control supplier change requests including bank details  
Ensure Delegation of Authority Plan (DOAP) is up to date and procurement duties properly segregated i.e. segregate:  
- requesting and establishing specifications from the procurement action  
- technical evaluation from financial evaluation of tender responses  
- managing the procurement action from awarding the contract  
- ordering from receipting from payment  
Stress importance of compliant procurement actions and enhance awareness of procurement procedures and the difference in emergencies  
Train supply and requesting personnel and procurement committee members on required procurement practices and ethics, as well as SOPs  
Ensure acceptance of goods / services according to PO and contract payments |
| **Consequences** | Principles of competition, fairness, integrity and transparency are compromised  
UNHCR or its partners may suffer reputational damage and face critical audit opinions  
Donor confidence in UNHCR may be negatively impacted and funding affected  
Financial loss, best value for money not achieved  
Compromised / reduced quality goods, services or works may be received  
Goods, services or works which are not required are procured and paid for  
PoCs may not receive goods and services as planned and resort to negative coping mechanisms  
Market may be negatively affected if other suppliers suspect lack of transparency or bias by UNHCR or its partners and lose trust, impacting future procurement actions  
Relations with host authorities may suffer  
Compromised UNHCR or partner personnel become more susceptible to repeat fraud or corruption  
Working environment becomes “toxic” and threatening, and in extreme cases dangerous, leading to curtailment of programmes or departure / withdrawal of personnel |
| **Reactive treatments** | Report any suspected fraud or corruption to IGO and support investigation as required  
Analyze poor tender responses to understand and document the reasons  
Enquire why a bidder withdraws or deliberately “spoils” a bid to understand and document the reasons  
Liaise with Vendor Ethics Committee (SMS HQ) regarding investigating a supplier suspected of fraud / corruption  
Institute appropriate sanctions against supplier following the decision of Vendor Ethics Committee after IGO investigation  
Collaborate and consult with Legal Affairs Service (LAS) before raising any legal claims  
Review with LAS options to terminate supplier contract  
Implement any personnel disciplinary measures determined by Human Resources  
Generally - support any formal investigations and implement required sanction as communicated by relevant authority without delay |

Note: further details of fraud and corruption risks can be found in the Procurement Risk Tool  
Note: the suppliers and personnel of a partner face the same procurement fraud / corruption risks noted above for UNHCR suppliers and personnel
Risk management tool: Fraud Prevention

### Causes
- Impression of impunity by partners’ and sub-contractors’ personnel
- Complex and changing environment i.e., an emergency
- Enabling environment for fraud and corruption
- Lack of access to operational sites and partner offices
- Insufficient monitoring of project implementation
- Lack of oversight, segregation of duties and rotation in UNHCR and with the partner
- Weak internal controls
- Partners and subcontractors unaware of what constitutes fraud and corruption
- Lack of focus on partner selection
- Partner’s heavy reliance on UNHCR funding
- False reporting or overestimation of needs, total population of PoCs, and identification of beneficiaries by partners
- Undeclared conflict of interest
- Uncertain personal situation and financial needs of partner personnel
- Lack of fraud awareness amongst UNHCR personnel

### Proactive treatments
- Review partner’s internal controls by using the Internal Control Questionnaire (ICQ)
- Recommend corrective measures for the gaps
- Ensure clear segregation of duties and responsibilities (through established SOPs)
- Ensure rigorous partner selection and retention process
- Perform spot checks as agreed with partner
- Ensure partner has anti-fraud and corruption policies and procedures in place
- Ensure partner personnel complete Fraud Awareness Basic Training on the Partner Portal
- Raise awareness and Code of Conduct training on fraud and corruption prevention & reporting among partner and UNHCR personnel
- Ensure risk-based monitoring, financial verification and remote monitoring, as needed
- Establish complaint/feedback mechanism(s)
- Ensure confidential whistle-blowing mechanism is in place
- Support integrity strengthening measures i.e., increase capacity building on operational delivery and oversight
- Collaborate with all stakeholders to combat fraud in the refugee response
- Establish common platforms and exchange information on assessment of partners on operational integrity, previous cases and common modus of fraud in the operation
- Ensure clear outcomes are included in Partnership Agreement with measurable indicators

### Consequences
- Misuse and/or diversion of aid if goods and services do not reach intended beneficiaries
- Objectives of partnership agreement not met
- Financial loss/payment against false or inflated receipts and invoices
- Financial implications, including the reimbursement of lost funds to UNHCR or donor
- Impact on future fundraising efforts
- Loss of stakeholder confidence
- Negative publicity and reputational damage for UNHCR and the partner(s)/sub-contractor(s)
- Poor audit reports
- Deterioration of relationship with partner and government due to the fraud case(s)
- Safety of UNHCR and partner personnel threatened
- PoCs receive sub–standard assistance/support services
- Suspension of activities impacting PoCs
- UNHCR inability to effectively fulfill its supervisory role

### Reactive treatments
- Report to Inspector General’s Office (IGO) fraud/misconduct
- Ensure close monitoring of cases referred to implementing partners for investigation.
- Review the quality of investigation reports submitted by partners
- Coordinate actions and external statements with DRRM, LAS, IGO in the event of the suspicion of fraud
- Escalate to regional bureau any cases of aid diversion, suspicion of fraud
- Request for audit of the project
- UNHCR/HCP/2015/5 - Policy and Procedures on Risk-Based Project Audit Certification
- Seek forensic auditing expertise if evidence of fraud/misconduct leads to significant, financial, operation and reputational risks
- Implement legal/punitive action, as agreed with relevant parties
- Terminate or non-renew the partnership agreement, consider direct implementation
- Depending on the agreed framework, inform the government on the available information related to the fraud allegation/case

Note: further details of fraud and corruption risks can be found in the Implementing with Partners tool
## Risk event | Fraud linked to undue influence on UNHCR processes by government authorities, donor countries and other entities

### Causes
- Partner imposed on UNHCR by external entity
- Corrupt decisions in the identification of project areas and activities (perpetuates ghost employees, receipt of commissions and income, unauthorized expenses, diversion of NFI or CBI)
- Issuance of permit to work and access to operational sites are used to influence UNHCR operations
- Authorized personnel or members of UNHCR decision making committees such as contract committees have undeclared ties to specific parties and/or are prone or exposed to pressure and influence
- Lack of diversity in the contract committee members or concentration of authority in limited number of personnel
- Oversight and controls on high-risk processes are not in place or not effective
- Limited possibility/access to carry out independent assessments and reviews
- Pressure and intervention on the procurement process to favour specific parties

### Proactive treatments
- Understand the local context, hierarchy, structure and culture of the operational sites to define threats, high risks, practices, tensions, biases, and other key considerations
- Train and increase capacity of personnel on how to prevent or effectively engage in activities that are potentially exposed to influential parties and malpractices
- Assign personnel with the right skills, experience and promote diversity in the operation. Ensure rotation of personnel
- Institute internal controls, oversight and governance processes on key activities
- Ensure regular review of processes and designation of authorities, roles and responsibilities
- Ensure effective inter-agency collaboration and sharing of information
- Ensure funding and partnership agreements are clear and free from biased conditions

### Consequences
- UNHCR operations impeded
- Deterioration of relationships with the different parties in the operational sites
- Harm and insecurity to personnel, assets and premises of UNHCR
- Disturbance in the operations, impacting protection and assistance delivery
- UNHCR’s independence and impartiality put in question
- Financial loss, potential harm to UNHCR’s reputation
- Loss of donor trust

### Reactive treatments
- Seek support from the host government
- Engage and seek resolution with the specific party, ensuring that host government is involved/informed, as needed
- Secure the personnel, asset or premises under threat or affected
- Provide immediate support to impacted personnel and strengthen personnel welfare initiatives and support, if needed
- Re-assign personnel if required and where possible
- Escalate to regional bureau and headquarter entities, as required
- Seek advice from LAS and IGO
**Risk event | Fraud in distribution of NFI's and provision of other services to PoCs, including Cash Based Interventions (CBI)**

### Causes

- Lack of understanding by the PoCs of their entitlements, the process and guidelines on the provision of services and goods
- Lack of proper targeting and verification
- Falsified information and documentation by third parties or PoCs leading to false information in the PoC database
- Insufficient documentation/data on PoCs
- Limited capacity in assessment, distribution, monitoring, oversight and reporting (UNHCR and/or partner)
- Services/supplies/package for PoCs attracts misrepresentation of information by the PoCs or other parties, such as splitting families, "borrowing" children and adding family members to inflate family composition to receive assistance
- Weak controls and system to detect fraud and other malpractices in distribution and delivery of services
- Bribery or extortion by other parties towards refugees and other stakeholders involved in the distribution
- Only one service provider available for CBI, giving them undue power

### Proactive treatments

- Ensure compliance with relevant UNHCR policies and operational guidance on distribution of goods and services, and CBI
- Institute systems in submitting and managing requests for delivery of services to PoCs to avoid intermediaries and exploitation
- Develop an anti-fraud strategy and action plan to strengthen detection and prevent occurrence of fraud in the distribution process (including identification of red flags)
- Ensure that PoCs’ database is regularly updated though verification and audit exercise
- Use biometrics and other automated systematic controls on recording and verification of data
- Collaborate with the Government and partners to put in place process in distribution and agreed framework on handling alleged cases of fraud
- Ensure segregation of duties for PoC data, targeting, distribution, and reporting
- Conduct capacity building and code of conduct dialogue (CoCD) sessions for personnel
- Raise awareness among PoCs and increase effective visibility regarding fraud/corruption and the consequences
- Establish an effective and accessible feedback mechanism such as hotline, outreach, etc.
- Use established financial intermediaries (cash providers) subject to national and local regulations and reviews

### Consequences

- Diversion of funds as those not qualifying receive assistance or the latter is diverted to third parties
- Needs of PoCs not met
- Fraud practices in distribution perpetuated
- Loss of assets and funds
- Reputational impact to UNHCR, government and partners involved
- Suspension/cessation of the activities benefitting PoCs
- Freezing of funds by donors
- Loss of trust by the PoCs in the UNHCR response/operation
- PoCs exposed to overly high withdrawal fees when withdrawing funds from cash providers

### Reactive treatments

- Remove individuals from beneficiary list, as needed
- Report suspected cases of misconduct for investigation and assist, if asked, the IGO
- Execute actions to recover funds, in accordance with the policy and agreement with relevant parties
- Re-evaluate effectiveness of controls and oversight. Institute revised controls to deter the re-occurrence of the specific risk/s that materialized
- Engage with donors to rebuild trust, and ensure information dissemination after execution of actions to improve integrity and accountability
- Review of existing contractual arrangement with CBI service provider

---

**Risk management tool: Fraud Prevention**
Risk event | Diversion of aid (financial resources, inventory, non-food items and other assets)

<table>
<thead>
<tr>
<th>Causes</th>
<th>Proactive treatments</th>
<th>Consequences</th>
<th>Reactive treatments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal, unauthorized and fraudulent practices by personnel, partners and other actors</td>
<td>Require potential partner to declare that it is not sanctioned by the UN Security Council sanctions list and that it does not directly or indirectly support entities sanctioned by a UN agency</td>
<td>UNHCR’s assistance and services not reaching persons of concern</td>
<td>Suspend contracts or partnership agreements concerned</td>
</tr>
<tr>
<td>Hostile, remote, conflict and/or emergency situation creates opportunities for diversion of aid</td>
<td>Require UNHCR personnel to answer questions on criminal, investigation and disciplinary records during the recruitment process</td>
<td>Objectives not achieved as PoCs needs are not met</td>
<td>Recover the diverted funds</td>
</tr>
<tr>
<td>Presence of militia, banditry (road/points of delivery)</td>
<td>Require PoCs to provide information on their identity at the time of registration that is verified on an ongoing basis</td>
<td>Material and financial losses to UNHCR against false/inaccurate distribution reports</td>
<td>Ensure investigation and imposition of disciplinary measures if warranted</td>
</tr>
<tr>
<td>Inadequate internal controls</td>
<td>Ensure thorough process in partner selection and retention, including vetting of partners and due diligence in registration</td>
<td>Reputational impact to UNHCR</td>
<td>Issue an official communication on aid diversion to host government</td>
</tr>
<tr>
<td>Lack of management oversight</td>
<td>Ensure partner contracts contain clause to report instances of funding diversion</td>
<td>Loss of trust by donors</td>
<td>Coordinate actions and any external statements with Donor Relations and Resource Mobilisation Service (DRRM), Legal Affairs Service (LAS) and Inspector General’s Office (IGO)</td>
</tr>
<tr>
<td>Insufficient documentation/data on PoCs, leading, inter alia, to overstated needs</td>
<td>Strengthen procurement governance, segregation of duties and closely respect/adhere to (do not override) automated controls in Enterprise Resource Planning (ERP)</td>
<td>Suspension of UNHCR operation and delivery of services</td>
<td>Report suspected fraud to IGO</td>
</tr>
<tr>
<td>Misreported or hidden, unauthorized expenses, inflated costs</td>
<td>Analyse key processes to understand potential for aid diversion</td>
<td>Sanctions by the government (persona non grata, cessation of UNHCR operations, expulsion of UNHCR from certain operational sites)</td>
<td>Engage with donors on the diversion of funds case, proving feedback and timely reports/briefings</td>
</tr>
<tr>
<td>Limited ability to carry out independent assessments, investigation, audit, and verification (e.g. due to lack of access, hindrance by third parties)</td>
<td>Organize fraud &amp; corruption prevention learning/training for personnel</td>
<td>Cancelation of partnership or deterioration of relationship with government</td>
<td></td>
</tr>
<tr>
<td>Insufficient monitoring of implementation, analysis of reporting and post-distribution monitoring (PDM)</td>
<td>Use biometrics in UNHCR registration of PoCs</td>
<td>NFiis/CRIs may end up in the hands of elements that are party to the conflict</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch to CBI through existing financial intermediaries that are subject to relevant international, national and local regulations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk event</td>
<td>Fraud in recruitment processes and career progression</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Causes** | Lack of verification of submitted documents by human resources (HR) personnel and / or management  
Cronyism or nepotism in the workplace (partiality in awarding jobs to friends or relatives)  
Abuse of authority / mismanagement by HR or other personnel  
Insufficient HR capacity  
Conflict of interest situations due to pressure from family, tribal affiliation or government  
Weak internal controls in HR processes  
Insufficient management oversight (e.g. segregation of duties) over recruitment and career management  
Loosened internal controls (screening) in emergency situations  
Lack of awareness of local dynamics (e.g. tribal affiliations) in operational environment by international personnel  
High level of unemployment in-country, creating pressures for fraud |
| **Proactive treatments** | Enhance awareness of personnel and potential candidates on HR processes including conflict of interest situation  
Conduct necessary background checks prior to recruitment  
Propose where necessary changes or modifications to existing processes and/or guidance  
Ensure effective management oversight in the different stages of recruitment and promotion processes  
Ensure that there is segregation of duties in HR processes and internal controls are in place  
Ensure sufficient HR capacity based on projected demand  
Put in place an HR training plan including annual code of conduct dialogue for personnel  
Ensure that personnel with HR responsibilities have signed the relevant confidentiality agreement  
Ensure recording and documentation of the different stages of the HR process  
Conduct reviews of HR processes, particularly those assessed as high risk  
Ensure personnel is aware of “Speak–up” help line and UNHCR’s “Whistle-blower policy” |
| **Consequences** | Unqualified candidates hired or specific candidates preferred over more qualified ones  
Poor performance/productivity and failure to reach organizational objectives  
Non-optimal impact of programmes due to non-attainment of the objectives  
UNHCR’s reputation negatively affected  
Loss of trust in the recruitment and other HR process  
Deterioration of personnel morale, psychological impact and stress to personnel, and toxic work environment  
Increasing number of management reviews  
Complaints to the UN Tribunal |
| **Reactive treatments** | Escalate issues to Division of Human Resources (DHR) or regional bureau  
Report suspected cases to IGO  
Reassess performance of relevant HR processes and take corrective action, as needed  
Remind personnel about availability of “Speak-up” helpline |

Risk management tool: Fraud Prevention
<table>
<thead>
<tr>
<th>Risk event</th>
<th>Fraud in personnel benefits and entitlements including the submission of Medical Insurance Plan claims and in leave and absence management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Causes</td>
<td>Proactive treatments</td>
</tr>
<tr>
<td>Lack of segregation of duties</td>
<td>Ensure personnel is aware of relevant rules and regulations, including those related to personnel entitlements</td>
</tr>
<tr>
<td>Weak internal controls or override of existing controls</td>
<td>Institute a second layer of oversight including random checks, such as calls to hospitals and education institutions</td>
</tr>
<tr>
<td>Insufficient HR capacity to process and verify claims</td>
<td>Train relevant personnel responsible for the HR processes. Ensure qualified and trained personnel execute the tasks</td>
</tr>
<tr>
<td>Lack of knowledge about local conditions including local languages</td>
<td>Ensure segregation of duties, and effective delegation of authority. For smaller offices, consider country or regional support</td>
</tr>
<tr>
<td>Lack of awareness of rules/regulations by personnel</td>
<td>Automate the process and maintain sufficient audit trail</td>
</tr>
<tr>
<td>Perception of impunity</td>
<td>Conduct periodic compliance reviews</td>
</tr>
<tr>
<td></td>
<td>Carry out market research on standard prices of services and medical fees. Inform personnel on the process and share price ranges and locations of service providers</td>
</tr>
</tbody>
</table>

Risk management tool: Fraud Prevention
<table>
<thead>
<tr>
<th>Risk event</th>
<th>Fraud in personnel management related to travel, training and missions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Causes</strong></td>
<td><strong>Proactive treatments</strong></td>
</tr>
<tr>
<td>Weak controls and / or lack of segregation of duties in processing and authorizing travel, training and missions</td>
<td>Update relevant SOPs and disseminate them widely both internally and to external parties involved such as travel agents and other contractors</td>
</tr>
<tr>
<td>SOPs not established for travel, training and missions or not thoroughly implemented</td>
<td>Ensure that UNHCR is not exposed to liabilities in case of private travel and that appropriate SOPs and controls are put in place</td>
</tr>
<tr>
<td>Lack of oversight on travel, missions and training affecting personnel</td>
<td>Ensure separation of duties (authority) in the travel authorization process</td>
</tr>
<tr>
<td>Travel claims not properly reviewed and approved</td>
<td>Strengthen and test internal controls on identified weak points</td>
</tr>
<tr>
<td>Personnel unaware of rules regarding travel, missions and training</td>
<td>Establish a review process over a certain interval of time. For example, (1) contractors bills and receivables should be reconciled, (2) submission of summary report of field missions and (3) logbook and monitoring of training opportunities</td>
</tr>
<tr>
<td>Undeclared conflict of interest</td>
<td>Conduct awareness raising and advocacy on ethical conduct, abuse of authority, and conflict of interest. This can supplement the CoCD or be a separate initiative</td>
</tr>
<tr>
<td>Extortion, intimidation, and coercion, to or by personnel</td>
<td>Increase awareness among UNHCR’s partners and contractors with regard to UNHCR’s policy on travel, missions and training and other advantages</td>
</tr>
</tbody>
</table>
### Risk event | Fraud linked to the use of UNHCR’s assets, inventories and supplies

<table>
<thead>
<tr>
<th>Causes</th>
<th>Proactive treatments</th>
<th>Consequences</th>
<th>Reactive treatments</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNHCR’s vehicles, generators and other assets are used by unauthorized persons or activities not linked to UNHCR operations. Malpractices in fuel management (e.g., distributed or sold to unauthorized persons, personal use, etc.)</td>
<td>Train personnel in warehouse and inventory control techniques and processes. Train drivers and other designated users of assets. Invest in automated systems and controls to track / control / record the use of assets (such as vehicle tracking systems, FleetWave, fuel gauge and cards, inventory systems for spare parts, maintenance scheduling, online tools and apps, etc.)</td>
<td>Loss of UNHCR resources and funds. Diversion of UNHCR resources (fuel, funds, assets, supplies and inventories). Damage, impairment and loss of UNHCR assets. Loss of reputation. Loss of donor trust.</td>
<td>Retrieve UNHCR’s assets. Process claims for insurance or other recourse for recovery. Review and follow up on any unreasonable expenses and unusual wear and tear of UNHCR property. Verify reports of unauthorized use and irregularities. Report to the IGO or designated party, for investigation as necessary. Cancelation of contracts and agreements. Consult with LAS and relevant units in Bureau and HQ. Issue official statement from UNHCR (general or specific case, as appropriate). Review the internal control where the lapses happened for the fraud to occur to avoid recurrence.</td>
</tr>
<tr>
<td>Poor controls in access, use, locations of assets, including inadequate storage infrastructure or security of assets, poor segregation of authorities, manual processes, etc.</td>
<td>Increase security and infrastructure in UNHCR’s warehouses and other premises used to store. Ensure clear responsibility and accountabilities of assets maintenance and usage including appointing focal point/s. Review expenses and calculate reasonableness test such as km/liter usage, monthly and per unit consumptions, high and frequent insurance claims, frequent repairs and replacements, etc. Inspect in a regular but unpredictable manner warehouses and assets locations. Review documents records and systems’ regular and exception reports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poorly maintained asset records including lack or inadequate documentary trails on the movement of assets, use of obsolete and manual systems. Pressure from authorities and other parties that exert influence.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadequate personnel capacity or knowledge to implement asset management. Purchase of assets, parts or services not in conformity with UNHCR’s procurement and fleet management processes.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: further details of fraud and corruption risks can be found in the Inventory and Asset Management Risk Tool.
## Causes

- Ineffective and insufficient data protection controls and practices facilitating cyber attacks
- Insufficient personnel capacity in ICT and/or lack of adequate knowledge and awareness of ICT, cyber and data fraud amongst ICT personnel
- Inadequate or outdated ICT infrastructure
- Failure to invest in and sufficiently secure ICT systems against cyber-attacks allowing vulnerabilities to be exploited by threat actors (i.e. state-sponsored, hacking groups, and insiders/partners)
- Insufficiently trained workforce in cybersecurity, data protection controls, and proper system usage
- Catastrophic failure of ICT infrastructure at either central data centers or in field locations
- The DIST backup & recovery system is not consistent and comprehensive across all systems
- Existence of locally developed and maintained IT systems with inadequate security controls
- Failure to maintain accurate and up-to-date access controls to key systems

## Proactive treatments

- Assess and conduct tests of ICT systems and infrastructure’s integrity and adequacy
- Ensure sufficient in-house ICT expertise
- Train personnel handling ICT and data and enhance awareness of data security measures of all personnel
- Issue SOPs relevant to fraud in data management and protection and monitor compliance with relevant rules, regulations and good practice procedures
- Collaborate with government and partners on strengthening data and ICT integrity
- Ensure back-up systems are in place, ensure use of cloud technology through secure connections
- Scan, file and upload PoC personal data to E-safe cloud storage
- Flag any identified threats to systems to DIST/HQ
- Strengthen the security and access controls of distributed systems

## Consequences

- Theft, loss or alteration of sensitive data
- Operational data could be compromised, adversely affecting availability of accurate and relevant data needed to address the protection and assistance needs of persons of concern
- Confidential data of PoCs or UNHCR are accessed and utilized for fraudulent and malicious purposes. PoCs threatened, exploited or exposed to harm (i.e. blackmailing, extortion)
- Reputational damage to UNHCR
- UNHCR’s operation compromised
- Shutdown or impeding of UNHCR’s operation and delivery of services (service interruption)
- Loss or misdirection of UNHCR resources
- Relationship of UNHCR with partners, government and other entities negatively impacted
- Loss of trust by the government and PoCs on UNHCR’s processes and integrity
- Possible disclosure, theft or alteration of sensitive data and interruption of ICT services
- Inability to maintain the continuity of critical processes and capacity to implement mandate and programmes

## Reactive treatments

- Strengthen ICT expertise / capacity
- Escalate to Senior Management (HQ-DIST)
- Upgrade of the failing infrastructure
- Conduct investigation (in close cooperation with supervision by DIST) on a case-by-case basis and in coordination with other agencies
- Activate in collaboration with DIST/HQ Disaster Recovery Plans
- Report suspected fraud from UNHCR/partner personnel to IGO
## Opportunity | Success in collaboration to combat fraud with stakeholders involved in the PoC response

### Causes
- Engagement with all stakeholders to combat fraud and corruption risks
- Donors’ understanding and increased support to combat fraud in operations / countries where there are inherent fraud risks
- Aligned interest with government to address and mitigate fraud and corruption
- Collaboration with private and corporate sectors in adopting best practices in fraud detection and mitigation
- Partnership with the media in enhancing awareness and advocacy against fraud and corruption
- Shared platform with UN agencies and other organizations involved in the refugee response in terms of information dissemination, pooled resources in training and advocacy and establishing common standard and systems in addressing fraud
- Use of advanced tools, systems, applications and controls to effectively detect and mitigate the risks of fraud
- Grassroot organizations and groups (i.e. PoC representatives, host communities) actively participate in initiatives combating fraud
- Availability of feedback mechanisms, hotlines, and other means to report suspected fraud cases

### Proactive treatments
- Establish integrity briefings with donors. Provide timely risk information and updates on initiatives to strengthen operational integrity
- Conduct thorough fraud risk assessments in high-risk operations and provide key results to donors on the level of residual risks
- Conduct annual risk assessment and determine corresponding treatments for identified risks of fraud committed by PoCs, including robust prevention, detection and response measures
- Inform government interlocutors on UNHCR’s fraud policies. Collaborate on training initiatives and agree on reporting and investigation framework
- Include integrity matters while engaging with private sector and development agencies on activities that will benefit PoCs
- Establish platform(s) on information sharing and reporting
- Collaborate on capacity building initiatives
- Establish an inter-agency strategy and plan of action addressing fraud prevention
- Standardize common processes, government permits, importation processes, codes of ethics, and shared commitments
- Invest and train personnel and partners in the use of advance systems in payments (e.g. use of financial gateways and established intermediaries) and procurement (e.g. e-commerce, standardized contracts)
- Develop effective feedback mechanisms and automated reporting mechanisms / tools

### Consequences
- Fraud and losses of UNHCR’s funds avoided
- Cost effectiveness. Reduced duplication of initiatives and exercises, new opportunities for innovative approaches
- Strengthened trust by donors, PoCs, and other stakeholders
- Confidence maintained / enhanced in UNHCR’s protection, assistance and solutions activities
- Strengthened reputation and public trust
- Strengthened collaboration among agencies involved in the humanitarian response that can go beyond collaboration in fraud prevention

### Reactive treatments
- Develop lessons learnt and best practices that can potentially also be shared with other operations and organizations
- Issue a statement on the united stand against fraud with the different stakeholders, highlighting measures undertaken
- Explore further areas of collaboration and information sharing amongst stakeholders, including for training and capacity building initiatives linked to fraud prevention
- Based on the agreed reporting and investigation framework, pursue the investigation and eventual action and recovery if the fraud is established. Disclose the results, if possible (while maintaining confidentiality)
- Enhance communication with communities on issues linked to fraud prevention
- Ensure timely and effective response to reported instances of fraud and address identified areas of fraud vulnerability (jointly with stakeholders, where needed) to avoid recurrence of fraud. Verify the functioning and comprehensiveness of internal controls
- Mitigate or rectify the negative impacts to the PoCs in case fraud has been committed, as possible. Ensure PoCs are aware of feedback and reporting mechanisms put in place by UNHCR and stakeholders