Fraud reporting guidance for FCDO-funded grants

Contents

Scope of the guidance

This guidance note is aimed to support grant holders of UK Aid Match in understanding their responsibilities for fraud prevention in the management of Foreign, Commonwealth & Development Office (FCDO) funds. The guidance includes the definitions used in understanding fraud, the responsibilities of the parties involved in managing fraud and advice on the mitigation and investigation of fraud.

While this guidance is intended to provide support and guidance, ultimately responsibility for the management of fraud remains with the grant holder. This guidance should not be taken as a replacement for a thorough understanding of the fiduciary risks of operating in a high-risk environment, or well-designed systems of policies and processes for the mitigation of fraud.

It should be noted that, under large funds such as UK Aid Match, fraud is inevitable. The public nature of the funds, the amount of money involved, number of partners in the delivery chain and the high-risk environments in which the funds operate all add to the risk profile of grants. However, the FCDO and the Fund Manager work together with grant holders to:

- Minimise and mitigate the risk of fraud.
- Ensure that when fraud occurs it is reported immediately, investigated thoroughly, and that lessons are learnt for the future.

What constitutes fraud?

There are four principal areas under which fraudulent activities can occur in a FCDO-funded grant context. Any incidence or activity under these headings are classified with the umbrella term of 'fraud.'

- Fraud: An intentional act of dishonesty by one or more individuals with the intent of making a gain for themselves or anyone else or inflicting a loss on another. For example, ghost beneficiaries, falsification of documents.

- Theft: The taking of another person's property or services without that person's permission or consent with the intent to deprive the rightful owner of it. For example, theft by internal or external parties, armed robbery. Looting and mass theft are also considered to be fraud within the FCDO grant funded context.

- Corruption: The abuse of entrusted power for private gain. For example, demanding or accepting incentives/ payments from beneficiaries, conflict of interest.

- Misuse or mismanagement of funds: Any use of FCDO funds for purposes other than as approved by UK Aid Match for the applicable project, or in a manner that is otherwise inconsistent with UK Aid Match's stated objectives. For example, ineligible expenditure; expenditure outside of the approved budget tolerances; financial reporting errors, unsupported expenditure.

It is important to understand that any loss (or risk of loss) of grant funds or assets is considered as fraudulent by the FCDO, who operate a **zero-tolerance** approach towards corruption, fraud, and misuse of funds within UK Aid Match grants.

Common types of fraud

Examples of some common types of fraudulent activities that may occur within UK Aid Match grants include:

Fraud

- Ghost or ineligible beneficiaries: Beneficiaries are non-existent or do not meet the eligibility criteria for which the funding was awarded.

- Payment fraud: Intentional misrepresentation of financial information such as fictitious, inaccurate, duplicate, or unauthorised transactions and invoices, and unauthorised changes to the payment systems, for example, false or inflated time sheets for project-related staff cost and payments made to the wrong suppliers.

- Procurement fraud: Intentional misrepresentation of a material fact during the tendering process. Examples include price fixing, contracts awarded without robust and transparent justification.

- Contract fraud: Whereby goods or services are not supplied, are of inadequate quality or are not in line with the criteria on which payment was agreed.

- Travel and expenses, pay and other allowances: Personal gain made through abuse of internal systems, such as inaccurate, inflated, or duplicate travel and expense claims, overpayment of salary and abuses of flexible working time systems.

- Computer hacking and e-enabled fraud: Whereby unauthorised access to computer material or systems leads to actual loss or the risk of loss. For example, diversion of funds through payment to an unauthorised supplier bank account, copies made of organisational websites, fraudulent fundraising emails sent to donors or individuals.

Theft

- Looting or robbery: Attempting to, or taking, any asset (goods or cash) by force or threat of force.
- Theft of assets: The taking/stealing of assets or property without permission or consent, which includes the disposal of assets prior to approval by the FCDO.
- Theft of cash: The taking/stealing of cash funds without permission or consent.

Corruption

- Conflict of interest: Whereby personal benefit is made from actions or decisions made in an official capacity, including financial payments or other favours.

- Bribery, kickbacks and facilitation payments: Incentives to act in a certain manner in exchange for influence or action in return.

- Irregular recruitment and unfair dismissal: All forms of nepotism, cronyism and favouritism fall under this type of fraud as well as advertising fictitious job opportunities and any unjust dismissal.

Funds mismanagement and other

- Unsupported expenditure: Organisational spend on allowable goods or services for which adequate supporting documentation is not obtained or retained. Examples include a lack of timesheets to support staff time spent working on the project, receipts not being obtained for small purchases.

- Misuse of grant funding: Funds are not used as agreed, which includes ineligible or unapproved spend, the movement of funds between different budget lines and the misreporting of performance.

- Misuse of assets and information: Whereby goods or information are not used for their intended purpose such as supplying information to outsiders for personal gain, and the personal use of funded project assets such as motorcycles.

- Financial mismanagement: Any instances of poor financial management, including poor value for money, fall under this category.

Roles and responsibility

Fund Manager responsibility

It is the role of the Fund Manager, on behalf of the FCDO, to manage fraud prevention measure for the portfolio of grants as a whole. This includes identification, reporting, and oversight of the investigations into all reported cases. The Fund Manager is also responsible for ensuring that the FCDO funds lost to fraud are recuperated.

Where the Fund Manager identifies, or becomes aware of, actual or suspected fraud, the FCDO (including the Fraud Investigations team via reportingconcerns@fcdo.gov.uk), is informed as soon as practically possible, even if full details of the case are not available at that time.

The Fund Manager will ensure that every reported incident is fully investigated on a case-by-case basis by the grant holder and is ultimately responsible for ensuring the quality of the process. For investigations, should the grant holder be judged to have a conflict of interest in self-policing, or doubts exist over capacity, the Fund Manager will either conduct the investigation themselves or request an external audit from the grant holder.

Investigation and case updates will be regularly submitted to the FCDO counter fraud team until a satisfactory resolution can be reached and agreed, and progress against all fraud cases are discussed with the FCDO on monthly basis.

It should be noted that, only the FCDO can ‘close’ a fraud case once they feel a satisfactory conclusion has been met.

Grant holder responsibility

Both the FCDO and MannionDaniels adopt a ‘zero-tolerance approach’ to fraud. Given the context in which we operate in, instances of fraud or attempted fraud are expected. Regularly reporting all allegations, suspicions or identified incidents of fraud is encouraged and is not viewed negatively or as unnecessary as the reporting of fraud can demonstrate that grant holding organisations have sufficient processes in place to detect occurrences.

The Accountable Grant Agreement requires all UK Aid Match grant holders to report any loss or suspected loss as soon as they become aware of any actual, or allegation of, fraud, even if full details are not known at the time of reporting.

Reports should be made as soon as possible and should not be delayed until an internal investigation has been completed. This also applies if any concerns or suspicions of fraudulent misuse of funds are raised informally and relates to concerns within both the grant holder and downstream partners.

Mitigating actions

It is recognised that fraud will never be eliminated; however, to minimise the risk of fraud occurring, grant holders should look to implement robust internal controls throughout the organisation. These controls should be routinely tested to ensure that they are being complied with and revised and updated when gaps are identified or if a fraudulent incident occurs, to prevent a similar occurrence, and to address new emerging challenges; for example, combatting cybercrime related fraud.

Grant holders should ensure that risk prevention is a theme that runs through all policies and processes. Many of these controls are expected to apply universally and will be consistent across all projects, others however will be project specific and assessment should be completed prior to commencing any process to ensure fraud controls are appropriate.

Policies

Grant holders have flexibility of how they control fraud, and there is no 'one-size-fits-all' solution which is rolled out across the funds. However, for guidance, grant holders should consider the following policies and processes as part of good practice in fraud prevention:

Anti-Fraud, Bribery, and Corruption policy

The starting point for fraud prevention measures should be an overarching policy which sets out the organisation's responsibilities and processes concerning fraud prevention, including the prevention of money laundering and terrorism financing. As a minimum an anti-fraud policy should contain:

- A policy statement demonstrating zero-tolerance
- Definitions beyond just fraud
- Responsibilities of different set of employees
- Reference to law
- Specific rules covering accepting bribes/gifts, making bribes (facilitation payments), conflicts of interests (if not elsewhere covered), money laundering, terrorism financing
- Investigation process
- Disciplinary measures
- Link to whistleblowing policy and procedures
- Reporting to governance structures.

These areas may be covered in different guidance - for example, disciplinary measures are commonly included in the Staff Handbook - but all areas should be covered in some point of an organisations policy framework.

Careful attention should be given to the groups covered by the policy. A common error is to make a fraud policy applicable to staff members only, whereas organisations should also consider volunteers, consultants and the Board.

Case management of fraud

Prior to experiencing cases of fraud an organisation should have established a system by which cases transition through the process of reporting, investigation, remedial action and lesson learning. In addition, the creation of a fraud response plan will allow a standard process to be clearly outlined for all staff to understand. To support fraud case management, a register of fraud cases should be set-up, tracking the case management of fraud cases along all points of the process to resolution. Following resolution, cases of fraud should remain on the register to allow a historic record to be maintained and to support analysis and quantification of fraud risks going forward.

A frequent mistake is ignoring the need for a fraud register until after fraud has been reported, thus some organisations do not have this in place if they have experienced no recent fraud. It is strongly advised that this system is put in place in advance of need.

Risk register and risk management framework

Risk registers and supporting frameworks cover more risk than just the risk of financial loss. Best practice would suggest three main elements to this:

- Risk management framework: An overarching policy setting out the identification and control of risks, the need for registers and the flow of project level risks into a centralised organisational register.
- Organisation-level risk register: The risk register should aggregate the key risks that the organisations face.
- Project-level risk register: Each project should have its own risk register which reflects the project-specific risks and will feed into the organisation-level register.

Risk registers should be live documents and must be regularly updated and reviewed with active management of the risks. Each risk should be formally assigned to an owner who is responsible for monitoring and reporting on mitigations and ensuring that the register is updated for their specific areas. Prior to the commencement of any project grant holders should review the risks of delivery, this will encompass a wide range of risks but in all cases the risk of fraud should be included for each project.

It is unhelpful to an organisation, and insufficient for the FCDO, for there to be a box-ticking exercise where risk of fraud is simply noted. In completing the risk register organisations should complete a thorough assessment of risk posed by an individual project. Consideration should be given to the flow of funds, the partners involved, procurement, cash management, and the environmental risks, to ensure that a grant holder understands the risk of fraud for any project engaged in. This allows not only a comprehensive understanding of the risk, but also will inform the design of robust mitigating actions tailored to each project.

Whistleblowing policy

Whistleblowing can cover the reporting of any concerns in the delivery of UK Aid Match projects but most commonly will receive complaints which can be categorised in two ways: fraud and safeguarding.

A whistleblowing solution can be very simple to implement; for example, an email address which can receive any reports of concerns. To make this effective and operational however, there are several supporting measures which need to be implemented. Staff and associated personnel need to be aware of the whistleblowing contact information, this is the main purpose of having a whistle-blowing policy. Beyond just staff members it is important the third-party stakeholders are also able to report concerns, the most effective means of achieving this is to publicise the whistleblowing contact details on an organisation's public-facing website.

Whistleblowing is an important tool to use in the identifications of fraud but grant holders should be aware of how to react once a whistleblowing report has been received. The whistleblowing policy should fully detail the investigation process for all allegations and describe the measures in place to protect the whistleblower and maintain confidentiality.

Audit

There are different types of audits which may be considered when designing fraud mitigations for an organisation of a project.

All organisations of sufficient size will have a statutory requirement for audit of their annual financial statements, the principal objective of these audits however is to provide a true and fair view of the financial position of the organisation, as such they may be weak when considered as a means of fraud detection.

An operational and system-based audit can be undertaken to identify the risk of fraud within organisations. This is an independent, systematic examination of an organisation, or a specific function of department, to determine whether management is effective and efficient and if practices in place promote improvement. This type of audit can identify and address weaknesses to improve systems and can also be targeted to fraud prevention.

Some audit methodologies can be specifically designed to target fraud – for example, a forensic audit aimed specifically at the project would be more likely to identify fraud. Alternatively, if a partner is considered weak then the grant holder may consider the value of an audit targeting just the expenditures of this one partner. This risk-based approach towards audit design is likely to identify fraud more reliably, and can be tailored to be proportionate, and need not be conducted every year.

Inductions and training

Training of all staff members and associated personnel forms an essential part of fraud mitigation. Ultimately, the strength of preventative measures is not dependent on policies but relies on the understanding of individuals implementing those policies.

All individuals, of both grant holders and downstream partners, should undergo induction training, including training on fraud prevention and reporting. All staff should sign the organisational Code of Conduct at induction, and annual refresher training on fraud prevention should be provided to all staff with detailed records kept monitoring who has received training.

Policies of partners

Projects are frequently delivered by a lead grant holder working with in-country delivery partners. Grant holders should be aware of the risks involved in delivering through partners, because the FCDO has no contractual relationship with downstream delivery partners and, under accountable grant arrangements, the grant holder is liable for all fraud losses.

Grant holders should reflect that their own policies will not apply to downstream partners by default. Prior to any grant commencing, the grant holder should conduct robust due diligence on all partners in their delivery chain. This due diligence should include a review of the partners' own fraud procedures and associated controls. In principle these should be no weaker than the grant holders, and if they are found to unsatisfactory then the grant holder may opt to work to strengthen their partner, or to insist upon observing the grant holder's policies for the purpose of the grant.

Experience has shown that downstream delivery is the highest risk point of implementing a grant. These risks are something that each grant holder should take seriously during the assessment of risk and appropriate measures should be designed to mitigate and complete assurance over these risks.

Other supporting policies

As previously discussed, fraud mitigation and risk prevention should run through all organisational policies and processes. In addition to the specific fraud mitigating measures described above, other key policies should also support and reinforce the organisation's zero-tolerance approach to fraud, for example:

- Staff Handbook: The Staff Handbook/HR Manual may include a number of sections in support of fraud controls, including disciplinary measures, recruitment policies, etc.
- Recruitment Policies: These can potentially be included as part of any staff handbook. Recruitment should include a screening of any potential candidates to ensure there are no issues of concern in their background.
- Code of Conduct: Codes of conduct cover all expectations of ethics and behaviours for staff, and they are frequently a document which individuals must show specific assent to by signing. Codes should include statement reinforcing the organisations zero-tolerance approach to fraud.
- Finance Manual: The finance manual is a key document in the financial management of an organisation. Whilst typically it will not contain specific sections on fraud, it is essential that all policies and processes within the manual.

- Procurement policy: Procurement is a high-risk area in relation to fraud. A robust procurement policy will be important to all organisations to ensure that expenditures are made competitively and fairly.
- Others: Fraud should be a consideration when designing any organisational policies, including those not specifically mentioned here.

Common examples of mitigations

When designing and implementing internal controls to mitigate the risk of fraud, some common areas to consider include:

- Embed sufficient segregation of duty
  Design roles and responsibilities to ensure that no one person has the ability to order, authorise and pay for goods or services or administer beneficiary payments. Ensure that dual authorisation is required for all payment, including allowances for beneficiaries

- Implement a transparent procurement policy
  Ensure that your procurement processes are clear and transparent. Ensure that independent quotes are obtained and conflicts of interest are declared and registered. An authorisation matrix should be in place that defines the level of authorisation needed in-line with the value of purchases and clear criteria for selecting suppliers is in place and adhered to.

- Know your partner
  All grant holders are responsible for the behaviour and activity of their partners. Grant holders should carry out robust due diligence checks prior to engaging with partners which give assurance that partner internal controls are sufficiently robust and that they have the capacity and resources available to meet FCDO's compliance standards. During delivery of the project, grant holders should routinely and regularly monitor their partner activity and ensure that project expenditure is sufficiently validated prior to disbursing funds.

- Embed sufficient segregation of duty
  Design roles and responsibilities to ensure that no one person has the ability to order, authorise and pay for goods or services or administer beneficiary payments. Ensure that dual authorisation is required for all payment, including allowances for beneficiaries.

- Insist on and retain evidence of all expenditure
  Invoices and receipts should be obtained and retained for all grant holder and partner

spend. We appreciate that there are often situations where receipts are not available, for instance in remote locations or for small purchases. In this instance, self-receipts, authorised internally should not be allowed, and we recommend purchasing a small receipt book that can be signed and stamped by a supplier as proof of expenditure.

- Secure and regularly check assets and stock
  Ensure assets and other commodities are kept in a secure environment and carry out regular inventory checks. Checks should be carried out at intervals appropriate for the type of asset. We would recommend monthly checks for retained stock items such as pharmaceuticals, food stocks, training equipment and tools, and quarterly asset checks on other assets such as mobile technology (phones, laptops, ICT equipment) etc), motorcycles, solar panels and other project equipment.

  An inventory system should be put in place to ensure that items withdrawn and returned (if applicable) are clearly signed for and key holders should be limited. Petty cash should also be viewed as an asset and regular spot checks should be made on the cash balance in addition to monthly routine reconciliations

- Take a zero-tolerance approach
  Grant holders should ensure that an anti-fraud culture is instilled within and throughout their own and partner organisations. All staff (including partner staff) should be regularly trained on how to recognise fraud and confidential reporting mechanisms should be in place to encourage any suspicions to be reported. All reports, no matter how trivial they seem should be transparently investigated and appropriate and proportionate action is always seen to be taken where applicable.

- Reduce or eliminate the use of cash payments
  Utilise mobile money transfers or a form of cash transfer payments operated by a reputable financial agent where possible for beneficiary payments. All supplier and staff payments should be made by bank transfer. In relation to staff expenses reduce the need for cash advances by considering centralising the payment for accommodation and ensure that the staff travel, and subsistence policy requires all expense claims to be supported by receipts.

Using mobile money payments to reduce cash payments

The implementation of mobile money transfers as a mitigating action to reduce the risk associated with beneficiary payments made in cash, has become increasingly popular, but also presents its own set of challenges and this method of payment needs to be subject to robust control measures. Areas to consider include:

- Are the mobile money transaction costs prohibitive for beneficiaries?
- Do beneficiaries have private use of a Smartphone or is a phone shared by members of a household?
- Are the beneficiary phones capable of downloading the required App's to facilitate payments?
- Is the network coverage sufficient or will connectivity issues hinder the ability to operate mobile transfers (especially in rural/remote areas)?
- How will beneficiary data be verified to prevent errors in recording beneficiary telephone numbers?
- Does the beneficiary population have the capacity to send/receive/ read text messages or is training required?
- Is sufficient segregation of duties in place to verify beneficiary data?
- Is the recording of mobile money transactions transparent and can clearly identify what the payment is for?
- How will transactions be reconciled to individuals accounts to ensure that the correct amounts have been paid and are consistent to what has been authorised?
- Can the risk be transferred to a reputable financial agent to facilitate payments?

How to report fraud

Grant holders are responsible for reporting fraud to the Fund Manager immediately at the point of identifying suspected or actual fraud. This reporting should take place without delay. Reporting should not wait for investigation or confirmation of the fraud.

Grant holders can report fraud though one of the three methods listed below with options one and two being preferred:

1. Directly contacting the Fund Manager by notifying your nominated Performance and Review Manager
2. Using the Fund Managers anonymous, confidential and free to call reporting hotline, hosted by EthicsPoint. The link can also be found on the MannionDaniels, UK Aid Direct and UK Aid Match websites.
3. Directly reporting to the FCDO via their fraud and whistleblowing unit at; reportingconcerns@fcdo.gov.uk

These methods are the only recognised means of reporting instances, or suspicions, of fraudulent activity. Grant holders should not use other reporting mechanisms available such as flagging an asset as stolen or lost on an asset register, or within the quarterly report narrative.

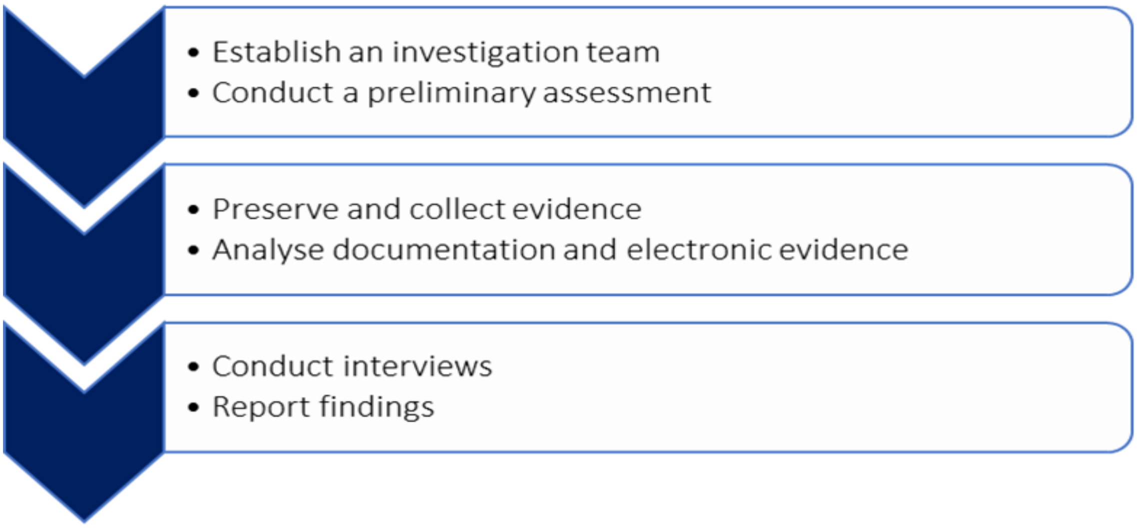
Grant holders are encouraged to complete and submit the ‘Fraud Reporting Form,’ when directly notifying the Fund Manager, a template of which can be found in Appendix 2.

Please complete this form with as much detail as possible, even if the full facts have not yet been fully established, as this will aid the reporting to the FCDO and enable the Fund Manager to quickly establish most appropriate course of action that will need to be taken. If there is information on the form which is not known at the point of reporting, please leave that section blank, completing the form should not be allowed to cause a delay in fraud reporting.

Use of this form is not a mandatory requirement when reporting fraud, however, should you choose not to use the form, we recommend that you familiarise yourselves with the content as it will give an indication of the key information you should look to include when informing your Performance and Review Manager.

How to investigate fraud

All UK Aid Match grant holders are expected to have their own investigative procedures in place, documented in their organisational anti-fraud, bribery and corruption policy. All allegations of actual, alleged, or suspicions of fraud must be thoroughly investigated in a timely fashion and should be treated as a fact-finding exercise to determine whether any fraudulent activity has occurred.



- Establish an investigation team
- Conduct a preliminary assessment

- Preserve and collect evidence
- Analyse documentation and electronic evidence

- Conduct interviews
- Report findings

In accordance with best practice, once an allegation or suspicion has been raised the following steps are recommended.

Once the findings have been reported, appropriate and proportionate action should be taken against the perpetrator which may include remedies such as issuing a written warning, suspension or dismissal from employment; pursuing legal action; terminating partner or supplier relationships.

Once the report has been finalised and approved, all grant holders are obliged to share the investigation report with the fund manager for review. Once satisfied that the investigation has been carried out conclusively and the decision reached is satisfactory, the Fund Manager will forward the report to the FCDO programme and counter fraud and audit teams for their final review.

Following the conclusion of the report, should fraudulent activity be identified, grant holders are also expected to carry out, and document a ‘lessons learnt’ report which identifies corrective action, with timelines for action, which should be taken to prevent future occurrences of similar incidents. This report, alongside the investigation report must be submitted to the fund manager to allow the FCDO to progress the case to closure.

Key steps of an investigation

The purpose of an investigation by the grant holder is to determine whether there are facts to support an allegation or suspicion of fraudulent activity and should be treated as an objective fact-finding exercise to determine whether fraud and loss to the FCDO has occurred. This guidance note informs grant holders of recommended best practice procedures to take once an allegation, or suspicion of fraudulent activity has been reported or raised.

1. On receiving an allegation or suspicion
   Fraud investigations typically begin following a formal allegation, which may be received from a wide variety of sources. It is estimated that 40% of all fraud detection comes from information being received from employees or external parties such as suppliers, partners and beneficiaries. In addition, potentially fraudulent activity might

be discovered during a routine internal or external audit.

The two immediate actions which must take place upon identifying suspected or actual fraud: report the issue to the Fund Manager and take any urgent action necessary to prevent further potential losses.

To account for the sensitivity associated with fraud allegations and to mitigate any potential fears of reprisal, grant holders are expected to have methods in place to allow both internal and external parties to report allegations anonymously, documented in a publicly available whistleblowing policy.

All allegations or suspicions that are received, whether written or verbal, should be clearly and accurately documented and swiftly shared with the appropriate parties for further investigation.

2. Establish an investigative team

   Regardless of the source of the allegation, the grant holding organisation should establish a team of individuals who have the appropriate expertise needed to conduct a successful investigation. The team can comprise both internal and external members, depending on the nature of the allegations, the magnitude of the potential financial risk or risk to the organisations involved and typical team members can include internal audit staff; finance managers; compliance officers; human resource personnel; senior management team members and external consultants with expertise related to the nature of the allegation.

   All investigation team members should have clearly defined roles and responsibilities and, in addition, at the onset of the investigation, the team should establish one primary point of contact. This individual will be responsible for managing the flow of communication and distributing information between all internal and external stakeholders during the investigation. Therefore, the point person should have an appropriate level of authority to make decisions on behalf of the organisation or in consultation with senior management. It should also be recognised that the appointed lead contact should be able to have sufficient time available to devote to the investigation, this may be considerable and could result in capacity and resourcing restraints which will need to be addressed.

3. Conduct a preliminary assessment

   Once the team has been established, it should quickly conduct initial enquiries to establish background information related to the allegation and should aim to:

   - Give an understanding of the context of the issue
   - Establish the identity of individuals with relevant information

- Establish the availability of evidence
- Define the organisation's end goal as a result of conducting the investigation.

Some typical questions the team might ask at this point in the investigation include:

- If the allegation is proven, whether the grant holder intends to pursue civil or criminal proceedings?
- If an employee is involved, can or will the grant holder (or partner organisation) look to terminate their employment based on the findings?
- Does the grant holder plan to file an insurance claim to recover any losses?

Answers to these and other relevant questions will aid the investigating team to develop a preliminary scope for the investigation. The scope may need to change as the investigation moves forward to accommodate information disclosed and issues identified during the investigation. The investigation team should ensure that the scope evolves over time and is regularly reassessed and updated accordingly.

4. Preserve and collect evidence

Once a grant holder has been made aware of any fraud allegation, it is important to take steps to preserve any electronic and hard copy evidence that might exist.

Examples of evidence include network files, or documents (such as invoices, receipts, data entry records, procurement details, bank statements, attendance sheets) retained within organisational information systems, hard copy files, email or other communications stored on company-issued assets such as laptops, mobile phones, tablets or desk top computers.

If an employee is implicated, steps for preserving evidence may differ depending on whether the grant holder or partner organisation plans to dismiss or suspend the employee or take no immediate action until the investigation is completed.

- If an employee is dismissed at the start of an investigation, efforts should be made to collect all company-issued electronic devices in their possession and secure these under the custody of the investigative team's primary point of contact. The employee's access to the organisation's network systems should be revoked immediately.
- If an employee is suspended / placed on paid administrative leave, their email and hard drive files should be backed up and stored securely.
- If no immediate action is to be taken against the employee and they are unaware of the investigation, efforts should be made to remotely access the employee's electronic devices to the extent they are available on company premises.

- In all instances, conducting a search of the employee’s office or workplace also is recommended.

5. Analyse documentation and electronic evidence

The investigative team should develop a comprehensive and detailed logical step-by-step approach to analysing all financial, organisational, and electronic records that are applicable to the fraud investigation. All records should be assessed for validity and compliance with patterns or trends being able to be identified. This may involve contacting suppliers or beneficiaries to establish whether funds or goods have been received in accordance with the evidence.

Investigative teams also should consider an effective approach to analysing electronically stored information. This type of analysis might be conducted in-house, if the capability exists or through a specialist, independent third-party that use software to extract and analyse data relevant to the investigation.

6. Conduct interviews

Interviews of witnesses and the subject under investigation should be carefully planned. It is advised that interviews are conducted after the majority of evidence and records have been assessed so that questions can be focused and evidence-based.

Prior to holding interviews, consideration should be given to the following:
- Should a human resource staff member be present during any employee interviews?
- Should an independent, appropriate adult be present during beneficiary interviews?
- When should the interviews take place?
- What is the appropriate order of the interviews – should witnesses be interviewed first?
- Who is responsible for co-ordinating the interview locations?
- Who will conduct the interviews, and who is responsible for keeping an accurate record of discussions?
- When should the interviewees be notified of the interview date?

7. Report the findings

When the investigation has concluded, it is important to consider the intended audience of the final written report. In addition to internal stakeholders such as senior management and Board members, external stakeholders such as donors, insurance companies or law enforcement agencies might require sight of the report to assess action to be taken if the allegation are proven.

Reports can be used to file insurance claims to recover losses resulting from the fraud and should the grant holder or partner organisation choose to pursue legal action, it is common practice to use the investigation report to refer the case to law enforcement. In addition, depending on the severity or complexity of the findings, local, state, or federal agencies might take an interest in the case.

In addition to the report, all original evidence should be logged and securely retained.

Appendix 1: FAQs

What is classed as 'fraud' for FCDO-funded projects?

The term fraud is used to cover any loss of FCDO funds or assets funded by the FCDO. This includes theft of cash or assets, lost items, purchase of ineligible items and any misuse of funding including ineligible expenditure or spend that has not been approved

Why is theft by external parties considered as fraud?

Theft or robbery by persons unknown or external to the organisation results in a loss of cash or assets. As this is a loss to the FCDO it does fall under the category of fraud and must be treated as such.

How should we report cases of/or allegations of fraud?

As soon as you become aware of, or have suspicions, regarding any loss or misuse of funds affecting your organisation, regardless of whether the FCDO funds are involved, you should either use the MannionDaniels confidential reporting hotline or inform MannionDaniels directly through your PRM. Mannion Daniels will, as fund manager, will liaise with the FCDO on your behalf to determine the next steps to take.

A grant holder Fraud Reporting Form has been developed and included in this guidance that can be used to document and report your concerns. This form will also be made available on the UK Aid Match website.

When should we report fraud?

As soon as you become aware of, or even have suspicions, regarding any loss or misuse of funds you should inform us immediately, even if you do not full details of the incident, such as the value of the potential loss, who is involved or how the loss occurred. This applies to all instances of loss or suspected loss that is affecting your organisation regardless of whether the FCDO funds are involved.

How do we investigate allegations, or occurrences, of fraud?

Following a report of fraud or suspected fraud Grant Holders are responsible for carrying out a thorough investigation and ensuring that appropriate action is taken against the perpetrator. Only under exceptional circumstances would the fund manager look to carry out the investigation themselves or utilise the services of an external audit consultant.
The investigation should be carried out in accordance with requirements of the grant holders own anti-fraud policy and should establish the nature of the incident, how this occurred, the value of any loss both to the organisation as a whole and to the FCDO – if applicable, plus the outcome of the investigation.

You should also include a 'lessons learnt' report which details the reasons the fraud occurred and mitigating actions (with timelines for implementation) to prevent similar incidences re-occurring.

Can funds be made available to cover the cost of investigations?

The FCDO expect grant holders to cover all costs associated with fraud investigations.

Appendix 2: Fraud reporting form