ASAP WEBINAR

ON

FRAUD: PREVENTING, WHISTLEBLOWER PROGRAMS, DETECTING, REPORTING, INVESTIGATING AND MANAGING CASES

JULY 29, 2020

Questions and Answers

ACCELERATING SUPPORT TO ADVANCED LOCAL PARTNERS (ASAP)

Fraud: Preventing, Whistleblower Programs, Detecting, Reporting, Investigating and Managing Cases

1. How do we verify whether somebody committed fraud knowingly or unknowingly?
    - When you ask "verify" I think this might delve into the investigation realm, and the need to know or document possible intent. This could lead to the classic question of "what did you know (or do) and when did you know it (or do it)?" But simple analysis of the activities that took place around a fraud, such as the dates of signoffs, approvals, payments, reconciliations, and finally, management review and approval, should flush out the reality of what transpired. Either way, as a prime recipient, it remains important to notify your AO and the OIG when you learn that a fraud took place.
2. Will you discuss "fraud" examples around vouchers (double billing?), kickbacks (vehicle repairs, travel agents etc.), and what to do when suspected-- how to properly investigate and how to avoid these or find them?
    - What will serve you best is to review and document this business processes from end to end including the information flow, systems used, manual records, and internal controls ranging from approvals, reconciliation and verifications. From there perform a risk assessment to document your inherent risks and then document what internal controls you have, access the likelihood and impacts of residual risks and take the appropriate adjustment to internal controls including but limited to segregation of duties, frequency of verification checks before approving transactions and reconciliations, etc. Continuously monitor this risk assessment and adjust at the working environment evolves including people, processes, technology and external factors. Documenting this is key for you to understand the circumstances to make informed decisions.
3. Does decision making after discovery of fraud depend on whether fraud was committed knowingly or unknowingly?
    - If fraud was committed regardless actions should be taken once detected. Fraud by definition is an intentional act to steal resources or cause damage to an organization.
4. Given the triangle factors that creates opportunity for fraud, what can be done to minimize fraud to a minimum or not at all?
    - Performing a fraud risk assessment tailored to the working environment is best. See the slide on the 5 step process and using the tool that's presented now. This allows you to document key risk indicators, likelihood and impact to them drive the decisioning making on the cost/benefit to implement preventative and detective controls including IT system controls and creating segregation of duties so not one individual control a business process transaction from end to end (e.g. creating vendor tables and approving payments).
5. What types of fraud will be committed at the subrecipient/local implementing partners level?
    - Common fraud schemes are improper fraudulent payments, including not performing services that the government is paying for, writing checks to individuals that should not receive payments, stealing equipment, etc.
6. Why do people commit fraud?

- It varies. Common motives include but not limited to their personal financial issues, pressure to perform, weak internal controls and process gaps that allows someone to commit fraud and they know someone won't find it to their beliefs, etc.

7. What is the scale of fraud? What are its significant risks during implementation of federal awards, in terms of cost and organizational reputation?
    - It varies based on the case and the dollar amount but also reputational impact, which is priceless which illustrate integrity and value issues that can be catastrophic to the organization. Weak internal controls in their financial business processes, competency issues and performance capabilities, pressure to perform, lack of segregation of duties, manual payments, etc. Lack of a risk assessment to document controls.
8. What percentage or portion were recovered from fraudsters?
    - It varies depending on each case which are too many to track. Normally it's low which why it's critical to document risk prevent fraud.
9. Who will commit fraud? Are executives and higher officials those who commit fraud?
    - Anyone who has motives to commit fraud, which varies on the individual's circumstances, therefore it's not limited to a group of people.
10. What substantial information/evidence is required to report fraud? Is only suspicion enough?
    - It varies but normally transactional evidence, observations, emails, suspicions based on some valid evidence, IT records of user activity, the person making big purchases, explained cash transactions, abnormal transactions, etc.
11. What are fraud indicators and warnings?
    - You will need to document a risk assessment to determine this based on your business and organizations operations. But there are documented fraud schemes ranging from stealing equipment, falsifying documents, making improper payments, not performing services that are being paid for, etc.
12. What are the principles for effective management of fraud?
    - GAO Fraud Framework. https://www.gao.gov/products/GAO-15-593SP
13. How can we deal with the fraud risk assessment?
    - Perform the assessment and implement control, identify gaps and develop corrective actions and continually monitor the assessment and update it at least annually and track corrective action frequently based on the outcome of the risk assessment. High risk needs immediate attention.
14. Who is primarily responsible to fight fraud in the organization?
    - Everyone in the organization.
15. What are anti-fraud risk response strategies?
    - When you document your fraud risk assessment this will inform you what internal controls are present and what additional controls are needed to be implemented.
16. Are local implementing partners expected to maintain anonymous web-based reporting mechanism to fraud?
    - Yes. it's highly recommended and should be communicated to USAID. If fraud is suspected it must be reported.
17. Is fraud decreasing or increasing throughout the world?
    - Significantly increasing.

18. For organizations who don't have an internal audit department/ risk committee, is it possible for each section/department to undertake a risk assessment for their units? Then have a comprehensive risk register for the whole organization.
    - Absolutely. Management of these sections and departments should be documenting their businesses from end to end to understand where the inherent risk are present to then implement the appropriate internal controls and continuously monitor the risk register and updates as people, processes, technologies and external factors change.
19. Does fraud identification have a time limit? For example, if in a five-year project you get information of a possible fraud case that might have happened four years ago, can you say it is late or register it as an identified case?
    - No, once discovered you should document the case and understand the root causes to implement internal controls and take the necessary disciplinary actions. If fraud occurs and you don't take action there's a high likelihood that it will occur again.
20. The Risk Map shows (among other categories) high impact but low likelihood risks; and low impact but high likelihood risks. Which of the two require prioritization in terms of prevention?
    - Generally speaking, all over it should be prioritized as high priority because it's about fraud. Fraud is very damaging and drives reputational damage. As you document the likelihood and impact, the manner of which you implement internal controls to mitigate the risk should then be prioritized as far as the time and cost it will take to do so. This includes and ranges from automated IT system preventative controls, the frequency of transaction reviews before making payments, reconciliations, etc.
21. What does detection by accident mean?
    - It varies based on the situation and the specific business process, such as when performing a financial reconciliation. As a part of the reconciliation you notice odd transactions or a person changing payee information and you notice the payment was rerouted to themselves and your vendor complains about not getting paid for their goods and services.
22. Frauds can generate internal conflicts within the organization. Do you need a protection mechanism for fraud alerts in order to safeguard a good working climate? May we have some alert system of fraud?
    - Yes. There should be a policy and procedure document and communicated to all employees and supported by management of the organization. Whistleblower protection is highly recommend to help prevent and report fraud. And any who reports fraud needs to be protected and their names should not be shared with the fraudsters only the investigators and the immediate management personnel and senior leaderships. Ideally report it to the OIG for independence.
23. Can poor employee compensation be a great risk of fraud? That's more cases of African non-profit organizations. The isolation of certain intervention areas constitutes a risk of fraud, close monitoring is a problem.
    - It's possible but it's more of a likelihood if the individual has a motive to commit fraud, such as access to sensitive information and their person financial situation.
24. CCtv is a deterrent measure?
    - Our question related to CCTV footage that has been recorded, meaning that it will only likely be reviewed after the fact which makes the observation of fraud detective.

However, as mentioned later in the quiz section, the fact that a possible fraudster knows that they will or might be caught, CCTV might/can also be deemed preventive. But also, knowing that CCTV footage will be taken, the fraudster may go to extremes to cover their faces, etc.

25. Can we say fraud has happened with an absence of an internal audit department in an organization?
    - Not always, management has the ultimate responsibility for mitigating fraud, employees can be empowered by participating in a robust risk assessment and implementing controls and performing those controls and reporting to management on a consistent basis and management taking the appropriate actions.
26. What actions do you take when someone has committed fraud unknowingly?
    - Committing fraud unknowingly is not possible. Fraud is an intentional act. Committing waste is possible with poor processes.
27. Are WB systems controversial--Apart from fears of non-confidentiality, non-action and retaliation?
    - I am not aware of honest employees ever taking exception to a properly set-up WB system. Dishonest management might find such systems controversial insofar as they might be caught for poor behavior.
28. What kind of protection should organizations put in place for whistleblowers to prevent victimization?
    - Whistleblowers will not be victimized if the process is water-tight anonymous. But this can sometimes be difficult if the information that was shared in the WB process could only have been known by one or a few staff members.
29. How do you know if a supplier manipulated or overpriced their invoice?
    - During our audits, we frequently perform "secret shopping" where our auditors call in, or visit the store, and price the same items that the organization purchased. Also, we look at the procurement process to determine who obtained the quotes.
30. Supposedly, the fraud is investigated and eventually found to be a mere defamation or blackmail. What should happen here?
    - If you can reach back to the person who blew the whistle or made the claim, you should explain to that person that you investigated their claims and based on the evidence that they provided, and any other information that you could gain access to, the issue did not raise to the level of fraud or theft or whatever the claim was. It is important that the claimant receives feedback, regardless of the validity of the claim, so that the system is perceived to be responsive. You might inform that person that if they have additional documentation or information that has not been shared, the issue can be revisited.
31. Is it advisable to hire someone who worked for a non-US organization and was dismissed due to alleged fraud but comes to join a US funded organization? Do you have a right to act on the hearsay?
    - I would suggest not acting on hearsay, but rather following up on any information you have and certainly perform reference checks or background checks, including hiring background check specialists which are available in many countries. You can also consider performing psychometric testing and other tests that may highlight less-than-

honest tendencies or traits. At the extreme, you could consider lie-detector tests. However, you will need to be careful (especially if you are hiring this person from the US) not to be seen to be discriminating against them. Check with the discrimination laws in your country.

32. How do you go about whistleblowing/reporting frauds committed by executives/senior management of an organization for those scared of the repercussions that could follow e.g. loss of job?
    - If top management is involved in fraud, and they often are, then you should consider determining who is on the Board of the organization. Depending on the size of the organization, they might have an Internal Audit function which reports independently to the Board. If no IA function exists, then determine if there is an audit and risk committee and report to the chairperson of that committee. If there is any possibility that the Chairperson of the Board, and the Chair of the Audit committee might be involved (which may be difficult for lower level employees to determine) then consider informing both of those positions and make it clear that you are informing both persons. Then, unless the entire Board is corrupt, some corrective action should be taken. If this is your situation, it is time to find another place to work as things will eventually blow up.
33. What happens with people who give false information and later we find out that it was wrong?
    - The WB program details or processes should be clear on what types of issues are covered by the program. This is defined at a high level in the USAID Mandatory Standard Provision. This is why I indicated that a good WB program should exist alongside of an Ethical Reporting program, which might deal with issues that are less severe that fraud or theft. But as noted in our answer to number 30 above, the organization must provide feedback to the claimant of what you found or did not find. There could be an analysis of the possible intention of the claim(s) to see if there may be an "agenda" against the person identified as the fraudster, and it you see any consistent or systemic "targeting" you, and or HR/management might look for other root causes.

ADDITIONAL QUESTIONS

1. In my experience working with LIPs in several countries in Africa, fraud is common and sometimes committed by CEOs. How can this be reduced as USAID moves towards achieving 75% of LIP as a prime by the end of 2020?.

- We believe that performing a thorough NUPAS assessment on the Organization component of the module, and reviewing the Internal Control structures can assist. Does the organization have an effective, active and diverse Board? Are the members of the Board independently appointed by the community they serve (e.g stakeholders), or are they friends of the CEO? How often does the Board meet? Can you examine the meeting minutes to see if substantive issues are addressed? Do Board members and management sign Conflict of Interest statements on a regular basis? Is there an Audit and Risk committee? Is there an Internal Audit function? Can you perform background

checks on the CEO before appointing him or her? Does the Board perform annual 360 degree assessments? As the COSO framework stresses, the "Tone at the Top" is one of the most important factors for a successful Internal Control framework.

2. Most Finance Officers do not report fraud committed by their supervisors, for fear of losing their job, and they end up compromising the act. How can this be addressed?

- As noted in a few answers above, a solid whistleblowing (WB) program where (hopefully) absolute secrecy is offered is the best way to address this. The finance officers need to be able to reach above the supervisors to the Internal Audit leader, or the Board officers who should be independent of management. If the Board Chairperson is truly doing his or her job, they should be willing to deal with any claims through the WB program. If you believe that the WB program is structured so that it does not reach beyond those who might quash the claims, then try to anonymously inform the Board Chair.

3. What happens to a whistleblower who reveals themselves because they regret having blown the whistle? Are they protected or can they be transferred?

- Good question. If the WB originally told the truth, and things were fraudulent, then they had done the right thing. Hopefully, the fraudulent system or person will be address. The WB should not have to regret having blown the whistle unless there could or would be possible retribution against this person. A good WB system protects the identify of all whistleblowers. So they should be "protected". If the system cannot protect them, and their identify must be disclosed, I am not sure that many organizations (or donors) will have any kind of witness protection program. This is why possibly confidentially communicating with the Board members (Chair) could result in some transfer which is not obviously related to any WB actions.

4. How effective can one report fraud detection when it' affect a superior person?

- Please see the answers to #32 and Additional Question #2 above.

5. What are the effective steps to take to report fraud incidence?

- If you are reporting through an effective WB system, having detailed information about the fraud will be essential. If you can supply documents, dates, emails, directly heard conversations, pictures, actual proof of fraud, this is helpful. While doing your best to maintain your anonymity, create some communication channel for the investigator to get back to you if they have any questions. Ask them for a phone number which you can call from a payphone or something not clearly related to you.

6. What are the precautions to take before reporting a fraud incidence?

- As noted in Additional Question answer #5 above, assess the confidentiality of the organization's WB program. Try to understand how independent the investigators are. If you believe that the organization's WB program is not really confidential or robust, you could reach out to the USAID OIG which is certainly independent. But in such cases, please make sure you double-check your facts and that the issue which you are reporting meets the criteria of the USAID Mandatory Standard Provision M22.