Enhanced Anti-Fraud Measures in High Risk Environments

This memo discusses enhanced anti-fraud measures that international NGOs can take to address the increased risks of fraud and corruption [1] when operating under emergency conditions, such as the current COVID 19 pandemic.

ENHANCED FRAUD DETECTION AND PREVENTION METHODS

Improved fraud reporting systems

Most serious fraud is detected by reports and many frauds cannot be proven without the cooperation of an inside witness. Most people are reluctant to report, however, unless they can be assured (1) of anonymity (2) that they will not suffer retaliation and (3) and that the victim organization will take action in response. It is senior management's responsibility to ensure that these conditions are met.

Install professionally managed whistleblower systems

Whistleblower systems should be well-publicized, professionally managed programs with expert operators, experienced in fraud detection and interviewing, The systems, which mostly rely on anonymous emails, should be available 24/7, not merely a telephone number in the HR department manned 9 to 5 with a voice message thereafter, as some organizations employ. Complaints should be promptly acknowledged and followed up by personnel experienced in anti-fraud measures.

Automated fraud detection systems, as described in some detail below, can be linked to whistleblower systems to promptly help evaluate the allegations. For example, if the complaint alleges bid rigging, the computer programs can quickly look for indicators of that offense in the bidding records. This procedure is commonly used by investigative agencies.

See much more information on how to respond to complaints and reports at https://guide.iacrc.org/how-to-respond-to-a-complaint/.

---

[1] These risks include kickbacks offered or demanded in exchange for the purchase of high priced, substandard goods, bid rigging to improperly steer contracts to unqualified bidders, again in exchange for kickbacks, bribes to inspectors to accept poor quality goods or works, collusion among suppliers to raise prices, the sudden appearance of "shell company" suppliers, fictitious vendors and other similar offenses.

The obvious, most immediate responses should be (1) more diligent background checks on employees and vendors, (2) more intensive, independent inspections of received and delivered goods and services and (3) close adherence to appropriate emergency procurement procedures.

HOW **NOT** TO RESPOND TO A WHISTLEBLOWER COMPLAINT

An international organization installed a complaint line in the HR department at its headquarters. It received a plausible, quite detailed anonymous email regarding a serious fraud in a project managed by one of the organization's satellite offices.

The organization ignored the complaint for months until other concerns surfaced about the project. It then attempted to reach the whistleblower whose cooperation was critical to resolve the issues. Not surprisingly, the whistleblower did not respond, and the organization was unable to collect sufficient evidence to resolve the fraud concerns.

EXAMPLES OF RELUCTANCE OF EMPLOYEES TO REPORT FRAUD WITHIN AN ORGANIZATION

Employees of several major international NGOs revealed in a confidential debriefing session that they were aware of serious fraud and corruption within their organizations that they neglected to report to senior managers for fear of retaliation.

In one case the employees were aware that the local Project Manager was meeting privately at night with local construction firms to award contracts without competition in exchange for kickbacks, and that the modestly paid manager was building a multi-million euro "mansion" 20 kilometers from the project site.

In another case, employees were aware that vendors were delivering grossly substandard goods and services in a huge refugee relief project, but neglected to report it. They believed the senior managers would resent being advised of the problem because it would adversely affect their relationship with funders. The employees also believe the managers would not take any action, even if informed, and that the reporting employee would be penalized for doing so.

There are many more such examples, and still more cases in which employees, auditors or investigators who included negative information in reports were told to remove it or were fired.

Exit interviews

Employees leaving an organization may be less reluctant to disclose negative information, assuming their

identity and confidentiality is still protected. The person conducting the interview should have some degree of fraud knowledge and a sympathetic attitude in dealing with whistleblowers.

Regular exchanges of information with other organizations

It is quite important to establish confidential channels to promptly share information on problem employees and vendors with other organizations in the same sector. On many occasions organizations victimized by fraud merely terminate the responsible employee or sever relations with the vendor,

allowing them to victimize other organizations. Systems to exchange such information is encouraged by some development agencies and funders. Check the legality of such exchanges in the country of operation.

Send "Christmas letters" to vendors

Notify vendors annually of the organization's ethics and conflict of interest policies, including the prohibition of employees accepting gifts from vendors. Ask the vendor to report – confidentially, if preferred - any misconduct by organization employees, including requests for gifts or kickbacks in procurement transactions, etc.

A CHRISTMAS STORY

A vendor replied to a Christmas letter by reporting that a senior procurement official employed of a large retail organization was offering to increase purchases from vendors in exchange for kickbacks. This led to an investigation that eventually identified hundreds of thousands of dollars of kickback payments to a number of procurement officials in exchange for millions of dollars of unnecessary, high priced purchases.

Conduct enhanced background checks on employees and vendors

It has been said, with some truth, that WHO an organization employs, and with WHOM it does business, is even more important than WHAT its controls system require. Background checks are exceptionally important in high risk environments.

Check for employees with undisclosed interests in vendors by matching employee contact information (address, telephone, email address) to vendor contact information. Include close relatives and emergency contact names of the employees in such checks.

Relatively simple supplier background checks can be effective to identify shell companies and phantom vendors:

- Does the vendor have a website?
- Is it listed in business and government registries?
- Address checks:
  - Is the vendor located at a non-business address? At a high risk address (e.g., in the US, a UPS office, a mail drop, an executive suite)? Is it located in a residential zip code?
  - Are there multiple vendors at the same address?

- Does the same vendor have two addresses listed for payments (possible indicator of a copy-cat phantom vendor)?
- Check social media sites on employees and vendors; note undisclosed relationships

If the vendors are in remote areas or too small to be listed in public databases, rely on confidential information from other organizations with experience in the region, as suggested above.

Discovery of a red flag of fraud

Fraud also may be detected by the discovery of a red flag - an indicator of fraud - by staff or auditors.

If a red flag(s) is detected:

- Match the red flag to the suspected scheme (training is usually necessary to do this; see examples of red flags matched to schemes at https://guide.iacrc.org/red-flags-listed-by-project-cycle/
- Look for other red flags of the suspected scheme(s); a number or pattern of red flags is more significant than a single indicator
- Determine if there are legitimate, non-fraud explanations for the red flag
- If not, or if it is difficult to determine, continue with further steps as necessary to resolve the issue, as set out at https://guide.iacrc.org/the-red-flags-of-corruption-bid-rigging-collusive-bidding-and-fraud/.

EXAMPLES OF DETECTION OF FRAUD BY THE DISCOVERY OF A RED FLAG

The award of a large contract to a single bidder, without adequate notice to other bidders, indicates possible bid rigging, which often is the result of corruption.

Bids that exactly match or are very close to the procurement entity's confidential cost estimates may indicate the leaking of confidential information to favored bidders.

Line item bids from different bidders that are identical or an exact percentage apart may indicate collusion by bidders and cartel activity.

Sequentially numbered invoices submitted by a vendor over an extended period of time (suggesting that the vendor has only one "customer") may indicate a phantom vendor set up by insiders to embezzle funds.

Computer aided fraud detection systems can be much more effective than human efforts, and can make possible "proactive" fraud detection measures: identifying and blocking possible fraud before losses are incurred. See the examples below.

Proactive fraud detection in purchasing transactions

A number of commercial products are available that can proactively detect or block fraud, waste and abuse in standard purchasing transactions. Most are installed in ERP or accounts payable systems.

SAP Fraud Management
https://help.highbond.com/helpdocs/essentials/6/user-guide/en-us/Content/global_topics/index.htm

Oversight Systems
https://www.oversight.com/
A 21-minute demonstration video can be found at:
https://insideanalysis.com/markets/operational-intelligence/oversight-systems/

AppZen (applies Artificial Intelligence to fraud detection and prevention)
https://www.appzen.com
https://www.appzen.com/blog/proactive-fraud-detection-the-future-is-artificial-intelligence-part-2/
https://venturebeat.com/2018/08/13/appzens-insights-uses-ai-to-automatically-detect-expense-reporting-fraud/

ACL (Galvanize)
https://help.highbond.com/helpdocs/essentials/6/user-guide/en-us/Content/global_topics/index.htm

Proactive fraud detection in eProcurement systems

Automated fraud detection programs that can proactively identify fraud and bid rigging can be installed in eProcurement systems. eProcurement systems, even without the addition of such systems, are more effective at controlling fraud and procurement abuses than traditional procurement systems.

Announcing that an organization is employing such sophisticated fraud detection measures (without disclosing, of course, the details of how they work) itself can be a deterrent to fraud.

Other Effective Anti-Fraud Measures

Do covert testing of controls

This would involve, for example, submitting knowingly false or inflated invoices for payment, or defective bids in tenders, to determine if existing controls would detect or block them. This procedure has been recommended by a major international funding and aid organization.

Include audit and inspection rights in contracts and major purchase orders

Such provisions permit the contracting entity to inspect the books and records of suppliers and contractors upon reasonable notice, without the need to obtain subpoenas or other orders requiring their cooperation.

Exercise of these rights is often a critical component to detect the payment of kickbacks, the submission of inflated and false invoices and the delivery of substandard goods and services. The rights should remain in effect for a substantial period of time after the implementation of the contract and permit access to the supplier's or contractor's financial records, as well as records that confirm compliance with contract terms.