Table of Contents

About Pact...............................................................i
Preface......................................................................ii
Introduction............................................................iii
1 Fraud defined.......................................................3
2 What makes an organization vulnerable?....................7
3 Consequences of fraud...........................................9
4 Fraud Indicators.....................................................11
5 Use of financial controls to prevent fraud................12
6 Use of non-financial controls to prevent fraud..........13
7 Detective controls...............................................14
8 The role of managers in fraud control.....................15
9 The role of the board of directors..........................16
10 The role of audit Committees.................................16
11 The role of law enforcement agents.......................16
12 List of appendices..............................................18
ABOUT PACT

Mission Statement
Pact’s mission is to help build strong communities globally that provide people with an opportunity to earn a dignified living, raise healthy families, and participate in democratic life. Pact achieves this by strengthening the capacity of grassroots organizations, coalitions and networks, and by forging linkages among the government, business and civil sectors to achieve social, economic and environmental justice.

Values
Pact’s mission is rooted in the following values:

- All people have a right to participate in decisions that affect their lives.
- Local communities should be the driving forces for their own social and economic development.
- Democracy grows out of grassroots participation and enterprise.
- Gender equity is mandatory for social transformation.
- Stakeholder inclusivity and power sharing inform Pact’s decision making.
- Relationships are based on a foundation of trust and respect.
- Programme design is client driven.
- Resource allocation choices are transparent and guided by sensitivity to the costs of operations, and financial accountability to our clients in recognition of Pact’s role as steward of resources intended for the poor.
- Enduring change defines the fundamental objective of all programme design.

PREFACE

The best practice series is a tool for organizations who are constantly striving to make things better. Organizations are very diverse, no two are alike. However, there are common lessons that can be learnt from one to another, and this series aims to share the knowledge which Pact has accumulated over decades of work in capacity building throughout the world.

The publications in the best practice series will give important inspiration on how management and staff can improve their organization’s performance, possibly through substantial rethinking. The series provides suggestions which can be applied directly in the organization, such as self analysis tools, guidelines etc, as well as overall discussion about the complexity of the issues raised.

Organizations are at various levels of development; therefore some will find more useful guidance than others in the series. However, experience has shown that even if a topic is acknowledged by an organization, there are sometimes many steps before it progresses from being acknowledged to being implemented right down to policies, administrative and financial procedures and program work.

Rene Hansen
INTRODUCTION
Fraud as an aspect of corruption normally happens in organizations where the governance structures are weak or have become corrupted themselves. This is a worldwide trend, which cuts across all sectors.

The Association of Certified Examiners of Fraud in the USA, define fraud as the “use of one’s occupation for personal enrichment through deliberate misuse or misapplication of the employing organizations’ resources or assets.”

The Collins English dictionary (1999) defines fraud as “a criminal offence in which a person acts in a deceitful way. Fraud can therefore be categorized as either internal or external.”

Everyone in the organization from the Director to the office technician has a role to play in prevention of fraud. Fraud can be controlled by CSOs through putting in place financial controls, non-financial systems and management oversight. Research has, however, established that reliance on internal controls and external audit are insufficient.

Fraud is recorded in the public, private sector and CSOs alike, but it is normally not publicized, and organizations deal with the problem internally. Accounts can be misrepresented and the information is usually internalized so that the donor is unaware of what is happening. CSOs normally work on a basis of trust and once this trust is lost then problems arise.

CSOs can misrepresent facts to the donor by misleading them about the impact of a prospective project. CSOs can also use the organization’s credit lines or cards to purchase goods and services for personal benefit. Individuals can fundraise for personal gain using the name of the organization.

Fraud is corrosive: if individuals find that they can get away with petty acts of fraud they will be tempted to try something bigger. Employees who see others getting away with corrupt practices will feel they are justified in pursuing their own. Risk assessment, awareness, control, deterrence and detection all have their part to play in the prevention of fraud.
FRAUD DEFINED

The Association of American Fraud Examiners conducted research in 2004 and established that the most prevalent fraud detection methods used in corporate and non-governmental organisations alike are as follows:

- Employees 51.7%
- Customers 19.7%
- Suppliers 15.7%
- Anonymous 12.9%

Major types of fraud
Fraud can be classified as internal when employees in a CSO identify an opportunity and commit acts of fraud. External fraud is committed when outsiders such as suppliers and service providers defraud a CSO, in some instances they would be working with internal staff. The following are various types and examples of internal and external fraud.

Factual misrepresentation
Facts about a cheque transaction can easily be misrepresented by an employee by altering the print to read a higher figure after authorisation and signature. The organisation’s accounts may be misrepresented by entering non-existent figures in the ledger. The employee can collude with suppliers to provide invoices with inflated prices.
Breach of trust
The head of a CSO is put in that position in order to serve the needs of the community or the stakeholders, and is thus expected to act for someone else’s benefit as a trustee. If the head decides to divert resources meant to benefit children in vulnerable conditions, in order to buy him or herself an expensive personal car, the fiduciary role is breached, and the Director or Coordinator has committed fraud.

Omission of critical facts
Critical facts in a transaction could be omitted by error or deliberately by an employee in order to benefit from the opportunity which could arise as a result. A staff member attending a fully-funded workshop can decide not to show the manager all the documentation relating to the expenses to be paid. The CSO could go ahead and process the standard travel allowances, accommodation etc, which eventually could be of personal benefit to the employee.

Bilateral donor engagement in fighting corruption in South Africa: misuse of donor funds
“Another much publicized case of the misuse of donor funds is that of EU support to the Department of Health for the AIDS play, Sarafina Two. After an inquiry by the Office of the Public Protector, donor money was found to have been allocated through improper tender and awarding procedures with a litany of irregularities involved in the spending of R14.2 million on the play. When the furore erupted over the extravagance of the project, the EU stated that it had never been asked to approve funds for the play contrary to assertions made before parliament by the minister of Health. The EU ambassador to South Africa stressed categorically that there had been no prior authorisation and regarded the diversion of funds as a serious misuse of EU support. In this case, there was no evidence or implication of the abuse of official position or titles for personal gain, but a clear case of diversion of aid in a manner bordering on mismanagement and a lack of both transparency and public parliamentary accountability.

The EU experience with the Department of Health has resulted in bureaucratic and regulatory consequences for organisations in South Africa, such as the Institute for Security Studies (ISS), which have received funds from the EU subsequent to Sarafina Two. Comprehensive accounting procedures are obviously necessary to regulate the use of donor funds, but stringency needs to be balanced with flexibility, particularly in relation to the policy work that organisations such as the ISS undertakes.……….."

Extract from Lala Camere’s article “ Anti-corruption Strategies Project, Institute of Security Studies, Cape Town, Published in African Security Review Vol.9 No 5/6,2000

Suppression of truths
The CSO can easily suppress information by reporting the progress of a project and taking pictures of non-existent structures and submitting these to a donor who is far away; whilst in truth nothing is happening on the ground. Critical receipts and vouchers may be destroyed deliberately to suppress the truth, or electronic information manipulated, in order to reflect what the CSO wants the donor to believe whilst the original accurate facts and figures have been destroyed.

What is internal fraud?
Internal fraud is when employees in an organisation are involved in fraudulent activities such as:-

Asset misappropriation
It is possible for staff and drivers to use the organisation’s cars for unauthorized activities or journeys. The telephone is one asset which can be easily abused by staff to conduct their personal business or social life.
Bilateral donor engagement in fighting corruption in South Africa: misuse of donor funds

“In South Africa, there have been some high profile examples of the misuse of donor funds within civil society and the state both before and after 1994. Examples include Swedish support for Reverend Allan Boesak’s Foundation for Peace and Justice where money destined for the victims of apartheid found its way into Boesak’s personal account. An amount of R726 000 earmarked for the production of 12 video cassettes on voter education and democracy were instead spent on building a studio for his wife. Boesak was found guilty of the theft of R259 000 and fraud involving R1.3 million from the Foundation for Peace and Justice and sentenced to six years in prison. His case remains before the Supreme Court of Appeal. The use of the term ‘struggle accounting’, devised by Boesak and others to stress that the secretive and corrupt nature of the apartheid regime made open and transparent bookkeeping of donor funds almost impossible during the struggle years, raises questions for donors. Can donors interact openly with civil society organisations in cases of severe oppression? What checks and balances can be put in place to prevent a situation similar to the Boesak case from arising?.................”


Revenue and cash receipt collection
It is common for people who work in the finance department, especially if they are given too much autonomy by management, to mis-appropriate sums of money. If the initiator of a voucher eventually approves and signs the cheque, there is bound to be temptation to abuse that trust. There is generally need to separate the initiator of a voucher from the final authority in order to minimize abuse. If an organisation receives cash at specific intervals, there is need to have a monitoring mechanism so that the collector of the revenue does not reconcile the cash against the receipts on his/her own.

Payroll and employee
If the opportunity arises, the human resources or Administration and Finance officer can maintain ghost employees in the payroll, with all the comprehensive employee personal details on file, in order to prejudice the organisation financially. This can be more easily done in organisations which are diversified with branch offices in different locations, and a full secretariat based at head office.

Stealing time from Employer
This is prevalent in organizations where salary payments are based on timesheets and there is transport available for staff to conduct routine business, either in the field or attending meetings in town. The timesheet requirement restricts employees from playing truant from work, but they can steal time in the above situations..

What is external fraud?
External fraud is when people outside the organization are involved in the abuse of assets and resources of a CSO.

Non-delivery of services
Prevalent in organizations which have centralized procurement policies. The employee develops a relationship with vendors for personal gain. An organization can be charged for the servicing of computers, cars, telephones, cleaning of carpets when the service has not been delivered. If management does not check services before payment, they are bound to lose a lot of money until the scam is discovered.
Fraudulent reporting on funds used
Field staff can overstate travel and subsistence allowances for their personal benefit, where the incumbent is required to account for the funds after expenditure has been incurred.

Fraudulent application for grant funds
A CSO can apply for an advance of funds from a donor on the pretext that the initial disbursement has been depleted on programme activities when there is very little progress done on the ground. The media has published stories of CSOs that have submitted pictures of structures under construction showing all the stages until completion for projects which are non-existent. The fraud is only discovered when the donor agency pays a visit or contracts evaluators to assess the impact of the project.

Inflationary Prices
An employee can collude with suppliers with whom a relationship has been established, to inflate the prices of goods delivered to the CSO for his or her personal gain. The officer can deliberately approach these suppliers whenever there is an item to be purchased, and endorse on the voucher that the identified company is the sole supplier of the product, in order to pass it on for payment without any questions being asked. This is detailed in the next paragraph, under procurement fraud. This is one example of the most prevalent type of fraud in organizations.

Procurement Fraud
There are different types of fraud registered in the sector. However the most prevalent is procurement fraud. Procurement fraud is a serious risk to a CSO. This is deceit perpetrated by an individual in order to gain unfair benefits or rewards whilst making purchases from external suppliers.

The fraudsters exploit loopholes and weaknesses in management procedures. In many cases personal expenses are classified as business expenses. This type of fraud is prevalent where a staff member has expenditure authority. If the initiator of a purchase has the power to select the suppliers, recommend the most appropriate, and initiate a purchase voucher, then an opportunity for fraud is created. The finance and administration policy should specify that the same person should not select suppliers, order and receive goods or process and pay invoices.

Procurement fraudsters often succeed in getting benefits from the purchase of office supplies, printing and marketing activities of the CSO. These activities normally do not attract so much attention as the core business. A risk assessment expert can easily identify typical scams, if the indicators are not obvious.

Fraud is also prevalent in the process of accepting, reviewing and evaluating proposals. An employee can assist a supplier to win a contract through the provision of confidential internal information about the bid.
WHAT MAKES AN ORGANISATION VULNERABLE TO FRAUD?

There are a number of factors which make an organisation vulnerable to fraud. Socio-economic factors are one aspect which can make a CSO vulnerable. Some of the major factors are highlighted below.

**Excessive control by founders**
Staff and board members might feel restricted in their actions due to a lack of autonomy and sense of ownership of the organization, so that levels of commitment and loyalties are diminished, leading them to commit acts of fraud.

**Failure to include individuals with financial oversight on the Board of Directors**
It is important to have at least one or two individuals in the Board who have a strong financial background, so that they can guide the decision making process at board level. These individuals should constantly check the work of the finance department and assist in developing the policy documents for the department, to make sure they are both preventative and allow for easier detection of fraud in the CSO.

**Nurturing of an environment of trust**
In most CSOs, employees are contracted on trust. The donors entrust their money to the heads of these institutions and hope that they will be accountable, and use the resources for the intended purpose.

Employees often undertake community work far away from the CSO offices, bringing progress reports to the programme manager who trusts that what is reported is accurate.

---

**Awareness**
Fraud in CSOs should not be treated as an internal secret never to be discussed lest the donor hears of it. Openness is the only way to get across the message that procurement fraud is not tolerated. An open and positive working environment will also help remove perceived workplace injustices that in most instances are the initial motivation for fraud. The manager should initiate awareness training and subsequently draw up a clear, written code of practice, covering such issues as acceptance of gifts and hospitality.

**Control of procurement fraud**
Trust is the cornerstone of employer-employee relations, and even effective employees can breach that trust. The manager should therefore strike a balance between trusting the employees too much and too little. Controls should be built into routine processes and be consistently applied.

Supplier checks should be thorough, to eliminate suspect suppliers. Check the invoice, e-mail, address and the Directors names on the letterhead. Investigate any suspicious linkages between suppliers and employees, business partners and contractors. Invoices need to be checked by random sampling, with specific checks of large one-off payments.
Some humanitarian organisations leave their implements or equipment with community members to use until the project has come to an end.

The CSO employees trust the community members to be responsible and accountable, by returning the implements or equipment in good order.

**Lack of job security**

In some countries working for CSOs is an admirable and attractive occupation, but in others it is no longer as gratifying as it used to be.

There are a number of reasons for this, ranging from restrictive legislation targeted at CSOs, single party autocratic government, donor fatigue and the presence of civil strife. Most employees working in such environments are tempted to engage in fraudulent activity, as they cannot make personal plans beyond the next two years at most.

Most CSOs operating in difficult environments have strategic plans ranging from six months to a year, and so the staff contracts may vary with the organisation’s planning strategies. CSOs generally employ younger people who may be starting families, or who have young families, and need financial security.

**Low staff remuneration**

Civil society organisations, believe that they are activists who are not concerned about monetary gain. Employees of CSOs are engaged with changing the social status of human kind and empowering them with human rights education so that they make informed decisions and choices.

With the current change in the economies and political dispensation of many countries, the cost of living is soaring and the risk associated with human rights activism is now too great so that staff feel the need for market related remuneration.

Unfortunately most CSOs in developing countries are unable to pay attractive salaries, particularly to local staff.

Source: Pact Kenya
CONSEQUENCES OF FRAUD

1 Weakens the financial position of a CSO, as programmes are abandoned midway and in some instances staff can go without salaries.

2 The image and reputation of the CSO are affected which has implications for future funding and strategic alliances.

3 If fraud is not detected in time, this can lead to the collapse of the CSO, as donors withhold their funds and staff leave while there is still opportunity for them to get jobs elsewhere.

Research indicates that there are certain factors present in almost all fraud cases reported, namely:

- **Intent**
  This is what distinguishes fraud from error or oversight in the accounting and financial reporting processes. The perpetrator would have thought about it and acted. The legal system also procedurally would want to establish intent during the trial in order not to convict an innocent person.

- **Motives**
  An employee may come under extreme financial stress, if she or he has health problems or family members are chronically ill. An employee may desire to solve a need or seek to attain a certain lifestyle. Possibly there may be gambling or alcohol-related problems.

- **Opportunity**
  Motives are translated into action when there is an opportunity to commit fraud. If that opportunity is not there, temptation is removed. Opportunity can present itself if a cheque book is kept in an unlocked office drawer, or a manager travels often and signs blank cheques for activities or purchases whose actual amounts are not yet available. This presents a great opportunity for the staff to tamper with the cheque book or the signed cheques. A manager can establish “opportunity” through studying the organisation and searching for weaknesses. An employee can omit a procedure once, and on realizing that no one has noticed, can skip the procedure in future, which can be used by colleagues to commit fraud.

- **Concealment**
  An employee who is committing fraud would obviously want to keep it a secret, but concealment tends to leave a paper trail, which is eventually discovered. Clandestine withdrawals from the CSO’s bank account can be detected if the CSO conducts
frequent bank reconciliations. Evidence of concealment can be detected if some of the following practices are observed:-

1. Maintaining a duplicate set of documents or electronic database;

2. Destroying documents like bank statements, vouchers and cheque stubs;

3. Recording non-existent journal entries in order to move fraud from one account to another;

4. Never taking vacation or sick leave so that no-one else undertakes your duties;

5. Restricting access to specific finance files through passwords or using personal locks, so that other staff in the same office do not have access when the incumbent is away.

**Rationalisation**

An employee may commit fraud but still invent a rational explanation as to why the fraud has been committed. This “rationalisation factor” encourages the perpetrator to continue committing the fraud. These are some ways in which individuals may rationalize their actions:-

“Some people do it, so why should I not do it too.”

“I will pay back the organisation later or I will stop soon since this is only temporary.”

“I get so little, but I work so hard, this organisation owes me.”

As a manager it is important that the detection mechanisms put in place should address opportunity, concealment and rationalisation. One such measure is a Risk Management Policy.

This policy normally would cover all sorts of risk in any CSO but the detail below relates to fraud and abuse.

The manager can engage experts including audit firms or insurance companies to make an assessment of the organisation by identifying the CSO’s potential risks of internal fraud and abuse. The experts can then recommend fraud reduction procedures and policies to be designed by the CSO.

Financial risk models may recommend taking measures such as comprehensive insurance, in order to transfer the risk of fraud away from the CSO.

Finally the organisation should have a level of financial exposure which they are prepared or willing to accept, in the event that fraud occurs.
FRAUD INDICATORS

There are various indicators as to who might be involved in fraud and these may be manifested through a change in behavior or physical appearance of an employee.

**Behavioural indicators**
An employee who always seems to stay at work a little bit later than everyone else or who wants to leave after the supervisor has gone.

A formerly outgoing employee who has become withdrawn.

An employee showing signs of drugs or alcohol abuse.

An employee who refuses to take any vacation or other time off.

**Physical indicators**
Signs of altered timesheets that a supervisor is requested to approve.

Signs of a correction or override made to stock count sheets or goods received vouchers.

Indications of photocopies or otherwise suspicious looking supplier invoices submitted for approval.

Signs of non-business expenditures incurred while on a business trip that are being charged to the organisation.

Everyone has a role to play in the control of fraud from the members of staff to the board of directors. There are three methods, which can be applied concurrently to detect and prevent fraud:

- **Use of financial controls such as policies and procedures applied in specific accounting cycles.**

- **Use of non-financial systems such as human resources processes of selection, recruitment and appraisals; Information Technology systems, insurance and risk assessment measures**

- **Management oversight such as the management and board of directors having a clear understanding of their roles and responsibilities.**

**USE OF FINANCIAL CONTROLS**
Financial controls are used to minimise the real or perceived opportunities to commit fraud and abuse, and secondly for management to be able to identify in a timely manner fraud that has been perpetrated. There are the policies, procedures and practices applied in specific accounting practices to ensure the integrity and related elements designed to achieve a variety of objectives.

Financial controls can be divided into preventative and detective controls; Preventative controls are meant to thwart...
fraud before it occurs and detective measures are meant to detect fraud and genuine errors that make their way through the preventative controls. Fraud controls can be applied in a number of ways, some of which are listed below.

**Income and receipt processes**
The member of staff who receives money or donated goods from members, donors and clients should not be the same person who prepares the vouchers for banking or warehousing of the goods. There should be an intermediary to check the income against receipts and pass these on to someone who does the banking or can check the accuracy of the documentation.

Cheques coming to the organisation should be immediately stamped and endorsed and may be recorded in an incoming mail book probably kept at reception. The received funds should be immediately deposited if possible. Otherwise money should be locked up in a safe. Where large amounts of money are involved such as conference or workshop payouts, there is need to hire a security guard, and examine the purses, bags and briefcases of staff.

The manager should make it standard practice that a record of all funds coming to the organisation is kept, with dates, payee names, amounts, purpose of payment and form of payment. A periodic reconciliation should be made of the intake record, with deposits made to the organisation’s bank account. There is also need to conduct a periodic reconciliation of the intake record with revenue recorded in the accounting records.

**Purchasing**
It is possible that an employee might not disclose a conflict of interest concerning a certain service provider. For example, the employee might award a contract to a relative’s company. This hidden interest is not in the interests of the organisation.

An employee might receive kickbacks from suppliers in exchange for approval to either order from or make a payment to them, when goods have not been fully supplied or are charged at a higher price.

Staff from the donor organisation can be bribed by a CSO manager, so that during the monitoring process some instances of non compliance are ignored.

**Payment**
Staff and external suppliers can be involved in this fraud. There should be a clear division of duties in the office so that there is transparency and accountability.

Fraud can take place when obtaining refunds for cancelled workshops, membership and subscriptions, or overpayment for services. Employees can design schemes whereby they duplicate payments to vendors and only deliver one cheque, converting the other to cash.
Most cheque tampering schemes involve forgery, altering payee amounts or creating duplicate or counterfeit cheques.

The CSO should put in place controls relating to who can sign a cheque and steps to be taken in approving a supplier’s invoice. Electronic transfer of funds from one account to another is easily accomplished.

**Payroll Processing**

It is important that the payroll is initiated from the finance and administration department with the manager reviewing and authorising the transfer of funds before pay slips are issued.

This assists the detection of fraud relating to unauthorised overstatement of hours worked in overtime, and the overstatement of pay rates without authority.

**Management of grant funded programmes**

The manager is accountable to the donor and hence has to institute controls such as making programme officers responsible for their project budgets which are monitored by the finance department.

**Expense Reporting Fraud**

In CSOs where there are benefits for payment of schools fees for dependants, access to fuel coupons, air fare and travel schemes, some staff members may overstate the number of children they have. Fuel coupons could be used by employees for other people’s cars.

Preventative controls should be contemplated for each step along the way. In some transaction cycles it is important to employ multiple measures.

Locks on filing cabinets – those cabinets should be kept in a secure lockable office or room, so that there is limited access to that room.

Use of passwords that prevent access to certain software applications - such as having a general windows password reinforced by passwords in the Pastel or Pay plus program, these two programs maintain the financial records of a CSO and information about the employees salaries and particulars.

Approval of all expenses and timesheets before payment.

A form can be designed internally to be used by all staff when initiating purchases and payments. This form should have at least three levels of signatures, initiator, authorizer and approver before it moves on to the next level of payment. Timesheets should be authorized by the immediate supervisor who then authorizes finance to pay the salary for that employee.

**USE OF NON FINANCIAL SYSTEMS**

Prevention and detection of fraud encompasses both financial and non-financial systems. A selection of the non-financial controls explained below can be applied in order to minimize the prevalence of fraud and abuse in an organization.
Hiring staff
During the hiring process the CSO should conduct criminal background checks, verify identification records, and have access to other records if possible, including credit ratings, driving records and traffic offenses and qualification verification.

Training
Staff development for the CSO staff should include awareness training about fraud, and this can provide vital information for the development of whistleblowers within the institution. Training can also provide staff with a greater degree of job satisfaction through the acquisition of new technical skills and qualifications.

Performance Evaluations
A standard system for the appraisal and evaluation of employees should be used so that employees do not feel disillusioned by the method used and react by harbouring fraud motives.

Security
Security over physical premises and confidential information should be tightened through the use of locks, passwords and restricting access to certain areas of the office and yard. The individual offices of the employees should be restricted to staff only and offices should have door locks. Safes should be provided, for valuables and cheques.

Information Technology Systems
There should be a policy in place to provide security for data transmission controls, particularly the server, with data input controls, including putting passwords on individual personal computers and limiting access to server files and modification of settings.

Insurance and Risk Assessment
An all-encompassing insurance and risk control cover should be in place, covering IT equipment, communication systems, buildings, staff and vehicles.

Communication systems
A policy for the access, use, and servicing of the equipment should be documented and institutionalized.

DETECTIVE CONTROLS
These are controls designed to catch frauds and genuine errors that make their way through the preventative controls. It is important to include detective measures as part of the financial controls to combat fraud and abuse. Detective controls might include:

Performing a monthly bank reconciliation, such as checking the ledger figures against the bank statements;

Reconciling actual results with expected results;

The manager insists on mandatory vacations, during which another employee performs the tasks
ROLE OF MANAGERS IN FRAUD CONTROL

Management has an oversight role in the implementation of the policies developed with the board. Some of the explicit roles of management are detailed below.

- Responding to and supporting the board of directors
- Development of policies dealing with internal control and fraud
- Establishing an anti-fraud culture throughout the organization
- Enforcement of all fraud related policies
- Taking corrective action relating to known fraud
- Establishing transparency and accountability
- Serving as a role model for every employee in the organization

Manager’s Role

The manager should aim to prevent as many types of fraud and abuse as possible within the constraints of time and money. There is need to design appropriate follow-up procedures to detect, in a timely manner, those acts of fraud that have been carried out successfully despite the preventive controls in place.

Source: Pact Tanzania

The anti-fraud tone should be set from the top and embedded in the employee handbook. Employees who see their managers behaving dishonestly will feel they have an excuse for doing likewise.

Heavy handed controls are likely to cause resentment and inefficiencies, and may even be counter-productive. On the other hand, management cannot turn a blind eye, even to trivial cases of fraud. Some CSOs have internal policies which have deterred staff from engaging in fraudulent activities.

The Danida staff code of conduct in Annex 1 is one example of prevention controls in an institution. The format can be adapted to local conditions.
ROLE OF THE BOARD OF DIRECTORS

- Serve as external liaison with external auditors.
- Direct the internal audit process.
- Manage conflicts of interest.
- Serve as a direct internal control in relation to the actions of senior management.
- Be spokespersons for the organization in relation to fraud committed by senior management.
- Select members to constitute an Audit Committee (3 to 5).

RESPONSIBILITIES OF THE AUDIT COMMITTEE

- Select and evaluate the organization’s external audit firm.
- Review and evaluate the scope and plan for the external audit.
- Review and approve the annual financial statements audited by the external audit firm.
- Monitor the adequacy of the organization’s internal controls.
- Receive and review all communications from the external audit based on generally accepted standards.

Technological development has added the new dimension of electronic fraud - “Internet Scams,” which are very difficult to prevent, and in most cases the NGO cannot recover the loss. The most prevalent are the Nigerian Money Offers, Auctions, and Lotteries. NGOs which have a desperate need to fundraise might find themselves falling prey to these scams.

ROLE OF THE LAW ENFORCEMENT AGENTS

There is not much literature on fraud and the law enforcement agents which has been documented. The term corruption is used to include fraud in most countries. This section would therefore touch on the legal instruments available in Southern Africa. Other regional blocs and countries have common legal instruments and protocols to deter fraud and corruption. An outline of a Fraud, Prevention and Theft policy is appended as a guide for those organizations who do not have similar written down policies.

FRAUD VS CORRUPTION

Fraud is the unlawful and intentional making of a misrepresentation which causes actual or potential loss.

Corruption is defined by UNDP as the misuse of public power, office or authority for private benefit through bribery, extortion, influence peddling, nepotism, fraud, speed money or embezzlement.


The levels in the quality of a country’s legal system vary, especially the chances of being caught and punished meaningfully for engaging in fraudulent activities.
Each country should have effective laws so that the credibility of the police and judiciary to act when notified of fraudulent activities in organizations is enhanced.

Deterrence and enforcement measures are valuable tools to fight fraud. It has been proved through experience and research that those initiatives which rely too much on punishment are unlikely to be successful in the long term and might even become counter-productive.

Southern Africa as part of a regional bloc has put in place a regional Protocol Against Corruption which was signed by the 14 countries of the Southern Africa Development Community (SADC) in 2001, by “reaffirming the need to eliminate the scourge of corruption through the adoption of effective preventative and deterrent measures and by strictly enforcing legislation against all types of corruption and fostering public support for these initiatives” (SADC, 2001).

The enactment of the protocol by SADC led some countries including Zambia and Tanzania to put in place nationally relevant Prevention of Corrupt instruments which also define corruption according to their context. All the definitions put across highlight the following as types of corruption, bribery, fraud, nepotism, extortion, embezzlement, graft and subversion of justice and good governance.

Law enforcement agents need to adhere to the country specific provisions of the corruption prevention/control legal instruments in their countries, investigate and advise the affected organizations on prevention and detection measures they can employ.

According to (Kunaka and Mashumba 2001) serious cases of corruption involving civil society organizations, public and private sector employees have surfaced in the SADC countries. In 2000, Zambian authorities received 674 cases of corruption, including fraud, 403 of these were investigated, 69 were prosecuted in court and 30 were convicted. These figures indicate how difficult it is to prove a case of fraud or corruption, hence the need for CSO managers to be alert at all times and prevent it before it occurs.

Source: Pact Ethiopia
BEST PRACTICE SERIES:

FRAUD PREVENTION HANDBOOK

ANNEX 1

MANAGER’S CHECKLIST

Fraud risk has escalated recently to the extent that 57% of organisations will have experienced fraud within the past two years (KPMG 2001). Management was found to be responsible for 21% of all fraud, and employees responsible for 57%. Implementing systems to protect your not for profit from the high cost of fraud must be a key consideration.

Credit card and expense account abuse, conflict of interest and purchase for personal use are the main types of fraud committed by management, with theft of plant and materials, misappropriation of funds and petty cash fraud the most common types of fraud committed by employees.

Lack of internal controls, or the lack of application and review of these controls, is the single greatest factor in facilitating fraud, followed closely by collusion between employees and an outside third party.

This Checklist has been developed to provide you with early warning signs that may indicate fraud is occurring, or has the potential to occur.

Analyse each of the following statements, indicate in the check box if you are concerned, and develop a strategy for action to neutralise the potential or real threat.

APPENDICES

Assets

☐ Do I have an asset register?
☐ Do I update it periodically?
☐ Do I have labels on the assets?
☐ Two employees update the register periodically

Cheques and Payments

☐ The originator is not a signatory?
☐ There are more than two signatories to the Account?
☐ Cheque payments are verified by Manager before dispatch?
☐ Cheque books always locked in the safe?
☐ Payments are only authorized when they have supporting documents?
☐ Do I have procedures to detect and report unusual payments?
☐ Do I have adequate information regarding financial performance?
☐ Are the explanations of budget variance adequate?
☐ Have my expense accounts suddenly increased?
☐ Do I defer statutory payments e.g. taxes
☐ Do I defer payment of insurance premiums for staff?
<table>
<thead>
<tr>
<th>Audits</th>
<th>Payroll and Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do I have an audit committee?</td>
<td>Do I have up to date Employee files?</td>
</tr>
<tr>
<td>Do I get a formal external audit and management letter?</td>
<td>The initiator of the payroll does not approve the salary payments?</td>
</tr>
<tr>
<td>Do I get qualifications in the auditors report?</td>
<td>Time sheets are authorized by the employee’s supervisor</td>
</tr>
<tr>
<td>Do I have a qualified accounting staff and Board treasurer?</td>
<td>Do I authorize transfer of funds before pay slips are issued?</td>
</tr>
<tr>
<td></td>
<td>Do I get monthly programme reports activities from branch offices?</td>
</tr>
<tr>
<td>Purchases</td>
<td>Staff</td>
</tr>
<tr>
<td>Do I have a procurement committee?</td>
<td>Do I have key staff resigning frequently?</td>
</tr>
<tr>
<td>Do I approve and authorize payments?</td>
<td>Do the employees indicate low levels of morale?</td>
</tr>
<tr>
<td>Do I check the delivered goods against the invoice?</td>
<td>Do I have a high staff turnover in the organization?</td>
</tr>
<tr>
<td>Do I rotate the staff who do purchases?</td>
<td>Is information flow delayed within the organization?</td>
</tr>
<tr>
<td>Are the duties of seeking quotes, ordering, making selection and</td>
<td>Travel and Subsistence</td>
</tr>
<tr>
<td>checking of delivery allocated to more than one individual?</td>
<td>Do I have an approved travel and subsistence policy?</td>
</tr>
<tr>
<td></td>
<td>Do I check the conference/workshop invitations before approval</td>
</tr>
<tr>
<td>Gifts and entertainment</td>
<td></td>
</tr>
<tr>
<td>Do I have a maximum amount to be given to visitors, donors etc?</td>
<td></td>
</tr>
<tr>
<td>Do I have a list of non gift items?</td>
<td></td>
</tr>
<tr>
<td>Do I have a list of questions employees are supposed to pose before</td>
<td></td>
</tr>
<tr>
<td>accepting gifts?</td>
<td></td>
</tr>
<tr>
<td>Do I have an approved code of conduct?</td>
<td></td>
</tr>
</tbody>
</table>
Revenue and Cash
☐ Do I have a cash box for petty cash?
☐ Do I have a safe or strong room for valuables?
☐ Do I bank cash on a daily basis?
☐ Do I always get financial reports on time?

ANNEX II
Sample of Fraud Prevention Principles in a Code of conduct

DANISH INTERNATIONAL DEVELOPMENT AID (DANIDA)
ANTI-CORRUPTION CODE OF CONDUCT

10 September 2004

Principles

a) Conflict of interest.
We will avoid any conflict real or potential between our personal interests and the interests of DANIDA. We will promptly report any occurrence of such conflict.

b) Misuse of official position and public resources.
We will not seek to influence for private purposes any person or body by using our official position or offering them personal advantages. Likewise, we will not use public property, facilities, services and financial resources for private purposes except when permission is lawfully given.

c) Respect for laws
We respect the laws of the countries in which we work.

d) Proper personal conduct.
We will ensure that our private conduct does not compromise our role as DANIDA employee.

e) Active and passive bribery
We will not give, solicit or receive directly or indirectly any gift or other favour that may influence the exercise of our function, performance of duty or judgment. This does not include conventional hospitality or minor gifts.

f) Anti-corruption
In accordance with the principle of “zero tolerance”, we are obliged to report suspicion or evidence of corruption committed by colleagues or others.

g) Openness and transparency as a rule – confidentiality when required. We will strive to achieve maximum openness and transparency towards our external constituencies. However, confidentiality will be applied when necessary to safeguard the rights of our partners, staff and others.

h) Non-discrimination
In our work we do not discriminate in respect of gender, colour, religion, culture, education, social status, ethnic belonging or national origin or any other status.

i) Dissemination of the Code
We will make our Code of Conduct known to our professional partners.
j) Observance of the Code
We will respect the principles of the Code and we will report any evidence or suspicion of breaches to the Code. The responsible superiors will ensure the legal rights and due protection of the whistleblower and the accused before, during and after any investigation.

Source: /www.ambbangkok.um.dk/ ANNEX III

OUTLINE OF A FRAUD CORRUPTION AND THEFT POLICY

1. Introduction
- Provide the profile of CSO and purpose of policy in a page.
- Definition of fraud, corruption and theft.
- Provide subheadings for each definition and give examples of each.

2. Prevention of Fraud and Related Crimes
- Section to address operational control presenting the related risk exposures and embrace related financial audit controls, personnel selection and monitoring techniques.
- Physical security that deals with visitor control.
- Systems security that concentrates on improper usage of computer systems, e-mail facilities, password control, authorisations, logging off, encryption and message authentication.

3. Conflict of Interest
- Explain what it is, and detail the channels to be followed by employees to disclose such information to management.

4. Relationship with members, stakeholders, donors and clients
- Detail on procedure for the divulging of information to outsiders and the acceptance of bribes, indicating the CSO’s stance on this and subsequent reprimand.

5. Gifts and Entertainment
- Provide a maximum amount to be given to visitors, donors, members and the individual responsible for the approval of the gift.
- Indicate those items which are considered to be non gifts by the CSO.
- Pose a list of questions an employee is supposed to consider when offered a gift so that they are certain that it is not a bribe.

7. Employee Responsibilities
- Impress the relationship of trust and the expectations thereof, what disciplinary action would be imposed on the employee.

8. Reporting of Incidents
- If employees become aware of fraud, where do they report, if there is a hotline, provide all the contact details including e-mail. A sample “Incident Report” format is appended.

9. Protection
- Illustrate how the employees who provide tip-offs would be protected by management.
10. Investigation and Protection
- This would indicate how these would be conducted internally, would it involve private investigation firms, undercover agents, handwriting experts etc, and what they would require from the staff.

11. Disciplinary Procedures
- Management obligations and responsibilities, if a fraud is uncovered in an organization.

12. General
- Could cover general issues of amendment, distribution, who ensures compliance to the document and the roles and powers of management and supervisory staff in monitoring compliance. The fraud report template can be appended to the main policy document and used to report cases of fraud.
ANNEX 3(a)

INCIDENT REPORT

<table>
<thead>
<tr>
<th>Reference</th>
<th>Last updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation</td>
<td>Date</td>
</tr>
<tr>
<td>Branch</td>
<td>Submitted by</td>
</tr>
<tr>
<td>Period of occurrence</td>
<td>Date of Detection</td>
</tr>
<tr>
<td>Title of Perpetrator</td>
<td>Approximate value</td>
</tr>
<tr>
<td>Perpetrator’s direct report</td>
<td>Original cost of loss</td>
</tr>
<tr>
<td>Recovery Prospects</td>
<td>Book value cost of loss</td>
</tr>
<tr>
<td>- from perpetrator</td>
<td>Replacement cost</td>
</tr>
<tr>
<td>- from insurance</td>
<td></td>
</tr>
</tbody>
</table>

Way detected: ________________________________________________

Name & title of detector: ________________________________________

Details of incident: ____________________________________________

Any other parties involved and/or suspected: ______________________

Any further irregularities suspected: _____________________________

Contemplated action to be taken to investigate the incident further: ________________________________________________
REFERENCES


4) KFM Consultants. Proceedings of Workshop, Fraud Prevention and Detection in the not for profit sector 17th February, 2005

5) www.fraud.org/tips/telemarketing

6) www.fraud.internet/general.htm

7) Report on the seminar on the formation of an independent anti-corruption commission, Transparency International Zimbabwe ,2001


9) SADC, Protocol Against Corruption, Gaborone 2001

10). www.ambbangkok.um.dk/