Fraud Audit Manual

Office of the Comptroller and Auditor General of Bangladesh

Fraud Audit Manual

(A manual to support an audit of an audited body's systems and procedures to detect and prevent fraud)

Preface

The Supreme Audit Institution (SAI) of Bangladesh always keeps itself abreast of the developments in the modern world of public audit. The present Manual is based on international best practices including ISSAIs. It may be mentioned that for the guidance of public sector auditors across member nations the INTOSAI -the global platform of the Auditors General issued International Standards of Supreme Audit Institutions, commonly known as ISSAIs in 2010. If these professional standards are followed in the SAI of Bangladesh, it will enhance the quality of our audits and help the auditors in playing their entrusted role.

While conducting audit, our auditors come across intentional distortions of financial statements and accounting records and/or misappropriations of assets which we usually call 'Fraud'. These used to be reflected and followed up as part of the usual financial or compliance audit process. There was no separate arrangement for fraud audit. The present Manual deals with fraud exclusively & is intended, inter alia, to support an audit of auditable entities' systems and procedures including internal control to detect and prevent fraud. It has also taken into accounts the practical experience of pilot audit conducted with the assistance of SPEMP-B Project.

This Fraud Audit Manual -the first of its kind in the SAI of Bangladesh since its inception in 1973, is an important deliverable under the current development project, i.e., Strengthening Public Expenditure Management Programme (SPEMP-B). International and national consultants as well as those who contributed to this valuable product deserve special appreciation. From now on fraud audit will be conducted as per this Manual and other audit standards. The Manual would help our auditors conduct fraud audit smoothly and efficiently.

The present Manual derives its authority from articles 128 and 132 of the Constitution of the People's Republic of Bangladesh and the Comptroller and Auditor General (Additional Functions) Act, 1974 and subsequent amendments thereof.

This Manual is a living document. It will be updated periodically. Any suggestion to improve it will be welcome. However, while applying the Manual, if any error or omission is detected or noticed, the matter may please be brought to the notice of the Office of the Comptroller and Auditor General of Bangladesh immediately for due rectification.

Masud Ahmed
Comptroller and Auditor General of Bangladesh

Dated: Dhaka, May, 2016

Fraud Audit Manual

Table of Contents

The manual also provides a template for carrying out the audit of audited body's procedures to prevent and detect fraud which includes a set of expected procedures based on a risk based approach.

An audit programme based on the template has been included in the manual (please see page 33).

Guidance on the other generic aspects of auditing including audit planning, performing the audit and gathering evidence, evaluating evidence and forming conclusions and reporting are provided in other OCAG manuals. This is in line with ISSAI 5700 which states that 'This guideline assumes the reader is aware of other relevant auditing standards and guidance'.

As a matter of good practice the manual ought to be modified by OCAG to make any necessary clarifications or changes in the light of general experience once in general use.

The report of the pilot audit has been included to provide a local context for the manual (please see page 39).

2. WHAT IS FRAUD?

Fraud is an intentional action by one or more individuals among management, those charged with governance, employees or third parties, involving the use of deception to obtain an unjust or illegal advantage[1]. So it may be committed by those within an organisation or by those outside of an organisation and may be committed by the management (who may be in a position to override established procedures) or by the non-management employees of an organisation.

There is currently no precise legal definition of fraud in Bangladesh although theft and offences relating to public servants are covered in the Bangladesh Penal Code of 1860.

For the purposes of this manual fraud may be considered as:

Theft - this is defined in Chapter XVII of the Bangladesh Penal Code of 1860 as 'Whoever, intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft'.

[1] Paragraph 3.8 of ISSAI 5530 and Paragraph 11 of ISA 240 in ISSAI 1240.

False accounting – this may be defined as dishonestly destroying, defacing, concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with intent to cause loss to another or furnishing information which is or may be misleading, false or deceptive.

Bribery and corruption–this may be defined as the offering, giving, soliciting or acceptance of an inducement or reward that may influence the actions taken by an authority, its members or officers. This is dealt with in Chapter IX of the Bangladesh Penal Code of 1860 which covers offences by or relating to public servants.

Deception – this may be defined as obtaining property or pecuniary advantage by deception and obtaining services or evading liability by deception – the latter includes tax fraud.

Collusion – this may be defined as any case in which someone incites, instigates aids and abets, conspires or attempts to commit any of the actions listed above.

The most common frauds are generally associated with assets misappropriation.

The theft of cash or other assets such as inventory items is one of type of fraud. Obtaining payment using fictitious invoices and payments to fictitious employees sometimes referred to as 'ghost employees' are the other types of frauds. The many various types of fraud schemes are covered in Appendix 15 which may be used to provide an awareness of the wide range of fraud risks.

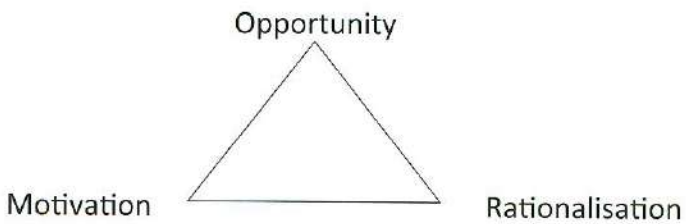
ISSAI 1240/ISA 240 states that: 'Misstatements in the financial statements can arise from either fraud or error. The distinguishing factor between fraud and error is whether the underlying action that results in the misstatement of the financial statements is intentional or unintentional. Although fraud is a broad legal concept, for the purposes of the ISAs, the auditor is concerned with fraud that causes a material misstatement in the financial statements. Two types of intentional misstatements are relevant to the auditor – misstatements resulting from fraudulent financial reporting and misstatements resulting from misappropriation of assets. Although the auditor may suspect or, in rare cases, identify the occurrence of fraud, the auditor does not make legal determinations of whether fraud has actually occurred'.

3. HOW FRAUD OCCURS

Four basic factors are necessary for a fraud to occur:

(i) People to carry out the fraud. They may be individuals within the organisation, outside the organisation or a group of people working inside or outside the organisation;
(ii) Assets to acquire fraudulently;
(iii) Intent to commit the fraud;
(iv) Opportunity.

The elements of fraud are also sometimes described as a triangle. The three legs of the triangle are opportunity, motivation and rationalisation.



Managers must ensure that the opportunities for fraud are minimised. While some people would never contemplate perpetrating a fraud others may if they thought they could get away with it. A high chance of being caught will deter. Opportunities to commit fraud may be reduced by ensuring that a sound system of internal control, proportional to risk, has been established and that it is functioning as intended. The purpose of the audit supported by this manual is to establish that such a sound system has been adequately designed and effectively implemented by management.

Motivation includes financial need, challenge and revenge.

Rationalisation is the final piece of the triangle. J R Dervaes has stated: 'It's not far behind the other pieces because this trusted employee is definitely at the centre of the organization's financial world. They're important, and they know it. Justification takes control of them as they proceed on this course of destruction. They've convinced themselves that they're entitled to the organization's assets, and feel no remorse about taking the resources either. After all, they're overworked and underpaid, and you owe them. Besides, they're already interpreted the organization's actions to mean that it doesn't care about the resources being

misappropriated anyway (rightly or wrongly, it makes no difference). In their own mind, they're right. They sleep well at night'[2].

Fraud indicators are discussed in section 4 below (fraud risk).

4. FRAUD RISK

Fraud is just one of many risks an organisation faces. However, the deliberate nature of fraud can make it difficult to detect and deter. Risk, in the context of managing fraud risk, is the vulnerability or exposure an organisation has towards fraud and irregularity. It combines the probability of fraud occurring and the corresponding impact measured in monetary terms. Preventive controls and the creation of the right type of corporate culture will tend to reduce the likelihood of fraud occurring while detective controls and effective contingency planning can reduce the size of any losses.

There are many fraud indicators relating to both the behaviour of individuals and unusual practices including for example unexplained wealth and reluctance to take leave and large payments to individuals and bank reconciliations that are not maintained or cannot be balanced. (See Appendix 13 for further fraud indicators). The risk of fraud is increased in the emergency phase following a disaster as set out in ISSAI 5530.

As discussed below assessing overall fraud risk is a key part of fraud risk management. The assessment includes ascertaining if among other things the audited body has a fraud policy statement and a fraud response plan and how the audited body demonstrates zero tolerance to fraud. (See Appendix 4 for a checklist for ascertaining if the audited body has adequately assessed overall fraud risk).

It is widely accepted that most frauds ought to be detected by the normal operation of the audited body's control procedures and by information provided by third parties.

[2] Fraud Manual by J R Dervaes ,Pp18

5. PILLARS OF FRAUD MANAGEMENT

5.1 Four Pillars

Prevention, detection, investigation and prosecution are considered the four pillars of fraud management. Each is as critical as each of the others if a fraud management system or initiative is to be successful in combating fraud.

Prevention Pillar – must detail how an organization will try to prevent fraudulent acts from occurring. It will assign responsibility for fraud prevention measures and hold those assigned the responsibility accountable of their efforts. Examples of fraud prevention measures include implementing an anonymous tip reporting system, conducting employment background checks and ensuring the physical security of assets.

Detection Pillar – is the second phase of fraud management. It involves a detailed detection initiative or systematic process of detecting fraud. At a minimum, organizations must designate and train staff to carry out fraud detection activities.

Investigation Pillar – brings the prevention and detection pillars together and provides evidence that either supports or refutes fraud allegations. Similar to the first two pillars of a fraud management program, organizations should clearly outline how allegations will be investigated and by whom. During the investigation pillar, predication must be determined to exist. Predication is simply a set of facts that would lead a reasonable individual to believe a fraud has occurred, is occurring, or will occur. Without predication, an investigation is not warranted.

Prosecution Pillar – is the fourth and final pillar in a system for combating fraud. Prosecution is the institution and conduct legal proceedings against a defendant for criminal behavior. A judicial proceeding commences and a determination of a person's innocence or guilt by due process of law results.

5.2 Inter- dependence of the Pillars

Prevention, detection, and investigation have little meaning unless there is a commitment to the prosecution of those who commit acts of fraud in government. The absence of fraud management system which does not encompass each of the four pillars of fraud management may indicate to the Internal Audit that management may not be fully committed to combating fraud, or that its efforts addressing fraud may need improvement.

6. AUDITING FRAUD RISK MANAGEMENT

6.1 What is Fraud Risk Management?

Everybody in an organisation contributes to the management of fraud risk. This starts at the top where senior management sets the tone of the organisation and promotes an anti-fraud culture throughout the organisation. Operational staff design and implement and operate the control actions required to minimise risk. The personnel function ensures that the right staff members are recruited. Accommodation services ensure physical security and IT services promote computer and data security. The role of internal audit is to deliver an opinion to the Principal Accounting Officer on the whole of an organisation's risk management, control and governance. In relation to fraud this will include the examination of the adequacy of arrangements for managing the risk of fraud and ensuring that the organisation actively promotes an anti-fraud culture.

The Principal Accounting Officer is responsible for maintaining a sound system of internal control that supports the achievement of departmental policies, aims and objectives, whilst safeguarding public funds and departmental assets. The internal control system should be designed to respond to and manage the risks which departments face in the achievement of their policies, aims and objectives. Managing fraud risk should be seen in the context of the management of this wider range of risks. The responsibility for the overall management of anti-fraud activities should be allocated to an appropriate senior officer.

As noted at paragraph 8.1.2 Internal Audit have a key role to play in the examination of the adequacy of arrangements for managing the risk of fraud and ensuring that the organisation promotes an anti-fraud culture.

A clear statement of commitment to ethical behaviour throughout the organisation should help to ensure that staff know that they are expected to follow the rules without circumventing controls and that they should avoid or declare any conflicts of interest.

Senior Management should try to create the conditions in which members of staff do not possess the motivation or the opportunity to commit fraud. The maintenance of good staff morale may help to minimise the likelihood of an employee causing harm to the organisation through fraud.

Under the right conditions staff members themselves are an excellent deterrent against fraud. There should be avenues for reporting suspicions of fraud. Staff should be encouraged to report suspicions of fraud either to their line managers, to internal audit or to a hotline set up for this purpose. The organisation's approach to fraud, which contributes to an anti-fraud culture, should be communicated throughout the organisation, including contractors and third parties delivering services on behalf of the organisation.

6.2 Auditing Fraud Risk Management

Auditing fraud risk management comprises auditing the two key components of fraud risk management:

- Fraud risk assessment (covered in section 7 below);
- Fraud risk assessment response (covered in section 8 below).

7. AUDITING THE FRAUD RISK ASSESSMENT

7.1 The Key Components of Fraud Risk Assessment

Managing the risk of fraud should be embedded in the entirety of an organisation's risk, control and governance procedures. A risk-based approach enables organisations to target their resources, both for improving controls and for pro-active detection, at problem areas. The key components of fraud risk assessment comprise:

- Assessing the organisation's overall vulnerability to fraud (covered in section 7.1.1 below);
- Identifying the areas most vulnerable to the risk of fraud (covered in section 7.1.2 below);
- Evaluating the scale of fraud risk (covered in section 7.1.3 below).

7.1.1 Assessing the Organisation's Overall Vulnerability to Fraud

Vulnerability to fraud can be assessed at different levels in an organization. A quick assessment of the overall level of fraud risk an organisation is exposed to is often a good starting point and may highlight particular vulnerabilities where some action needs to be taken immediately rather than wait for the results of a more in-depth risk assessment to be completed. In organisations where the risk of fraud is known to be high, a separate specific fraud risk assessment and evaluation may be appropriate.

Where the risk of fraud is considered to be low a specific fraud risk assessment may not be necessary, any risks being considered instead as part of the organisation's overall risk assessment. However, it will still be necessary for those organisations to develop an anti-fraud culture.

A fraud risk assessment should additionally be carried out during the development of any new policies, activities or operations to ascertain whether any new risks arise that need to be managed. The risk assessment should also be reviewed and re-assessed whenever a change in policy occurs or when changes are made to the way in which a policy is to be implemented.

7.1.2 Identifying the Areas Most Vulnerable to Fraud

The overall fraud risk review will show the scale and nature of fraud faced by the organisation and the relative risks between different types of fraud. This will determine whether there is a need to perform a more detailed assessment of those risks to provide a guide as to where the audited body should focus its efforts in improving control. This more detailed assessment of fraud risk will result in an "exposure profile" or fraud risk frame work that identifies the areas in which an organisation may face fraud threats and the types of threat it may face. It will not be cost effective to cover every possible threat situation therefore the likely occurrence of potential fraud, and the impact on key organisational objectives must be assessed. The steps in this stage include:

- identifying the processes or activities at risk of fraud. These can be identified using a number of techniques including:
    - commissioning a risk review;
    - undertaking risk self-assessment through: facilitated workshops and interviews; brainstorming; questionnaires; process mapping; and discussions with peers;
    - benchmarking – comparisons with other organisations.

- assessing and ranking the nature and extent of vulnerability in each area (Appendix 6 provides some common factors used to make judgements about vulnerability).
- identifying the particular forms of fraud threat to each area (Appendix 7 provides various examples of particular forms of threat).

7.1.3 Evaluating the Scale of Fraud Risk

In deciding how to handle the fraud risks identified in the exposure profile it is important to evaluate their significance. Risk evaluation and assessment will inform decisions about the areas of risk where action needs to be taken and the relative priority of those risks.

An analysis of threats against compensating factors such as internal controls is a key part of this task.

This phase of the risk assessment seeks to determine the extent to which existing internal controls are sufficient to counter the fraud threats that have been identified.

Once risks have been identified, an assessment of the possible impact and corresponding likelihood of occurrence should be made using consistent parameters that will enable the development of a prioritised risk analysis. Management should agree on the most appropriate definition and number of categories to be used when assessing both the likelihood and impact of each risk. The assessment of the impact of the risk should not simply take account of the financial impact but should also consider the organisation's reputation and recognise the potential political and commercial sensitivities involved. The analysis should be either qualitative or quantitative, and should be consistent to allow comparisons. The qualitative approach usually involves grading risks in high, medium or low categories.

7.2 Auditing the Fraud Risk Assessment

A template has been designed to focus the audit on the two key components of fraud risk management: fraud risk assessment and fraud risk assessment response as shown in Appendix 3.

For each of the three key components of fraud risk assessment set out below an expected procedure has been identified:

(1) There is an overall assessment of fraud risk;
(2) The areas most vulnerable to fraud have been identified and assessed; and
(3) The scale of fraud risks has been assessed taking into account the strength of internal controls.

The audit will comprise checking that the expected or equivalent procedures have been adequately designed and implemented for the purposes of preventing and detecting fraud.

Techniques for gathering evidence:

As referred to in paragraph 97 of ISSAI 4100 evidence may be gathered using a variety of techniques such as:

a) Observation
b) Inspection
c) Inquiry
d) Re-performance
e) Confirmation

Examples of test procedures have been included in the template- they are generic and may have to be adapted to the circumstances of a particular audited body.

The template also provides the facility to record a summary of the evidence obtained and a summary of key conclusions and recommendations.

As referred to in paragraph 93 of ISSAI 4100 the sufficiency of evidence relates to the quantity of the evidence. The competence, relevance, reliability and appropriateness of evidence relates to the quality of the evidence. Public sector auditors exercise professional judgement in making the determination of sufficiency and appropriateness throughout the evidence gathering process.

Also, as required by ISSAI 100 regarding the fundamental principles of public sector auditing auditors should maintain appropriate professional behaviour by applying professional skepticism and due care throughout the audit.

Sections 1-3 of the pilot audit report provided on page 39 cover the results of the auditing of fraud risk assessment of the audited body.

8. AUDITING THE RESPONSE TO THE RISK OF FRAUD

8.1 The Key Components of the Response to the Fraud Risk Assessment

Once the risks have been evaluated and prioritised consideration can be given to identifying appropriate responses. Responding to the risk of fraud involves compiling anti-fraud control policies and fraud response plans. Additionally it also involves putting in place effective accounting and operational controls and the maintenance of an ethical climate that encourages staff at all levels to actively participate in protecting public money and property. Responses to fraud risk include:

- Developing and promoting an anti-fraud culture (paragraph 8.1.1);
- Allocating responsibilities for the overall management of fraud risk and for the management of specific fraud risks (paragraph 8.1.2);
- Establishing cost effective internal controls to detect and deter fraud that are commensurate with the identified risk (paragraph 8.1.3);
- Developing the right skills and expertise required to manage the risk of fraud effectively and to respond effectively to fraud when it occurs (paragraph 8.1.4);
- Responding effectively to fraud when it occurs (paragraph 8.1.5);
- Establishing appropriate avenues for reporting fraud (paragraph 8.1.6);
- Continuously monitoring the risk environment and systems of internal control (paragraph 8.1.7); and
- Reporting fraud centrally (paragraph 8.1.8).

8.1.1 Developing and Promoting an Anti-fraud Culture

Fraud prevention involves more than merely compiling anti-fraud policies. It also involves putting in place effective accounting and operational controls and the maintenance of an ethical environment that encourages staff at all levels to actively participate in protecting public money and property. Creating an anti-fraud culture involves:

- Having a clear statement of ethical values;
- Establishing a clear anti-fraud policy (the key components of such a policy are covered in Appendix 10) and fraud response plan (the key components of such a plan are covered in Appendix 11);
- Promoting staff awareness of fraud;
- Recruiting honest staff (checking references etc.); and
- Maintaining good staff morale.

Code of Ethics

As stewards of public funds civil servants must have, and be seen to have, high standards of personal integrity. Staff should not accept gifts, hospitality or benefits of any kind from a third party that might be seen to compromise their integrity. All

personnel should be reminded that they are bound by a code of ethics which, unless issued separately, should be stated in the anti-fraud policy.

Please see Appendix 9 for further detail.

Fraud Policy

Many organisations use a fraud policy statement to communicate the organisation's approach to fraud. Such a statement may include some or all of the following areas:

- A statement about the organisation's attitude to fraud (e.g. zero tolerance);
- The Code of Ethics;
- Personnel policies (e.g. recruitment policies);
- The allocation of responsibilities for the overall management of fraud;
- Reporting suspicions of fraud, including "hotline" arrangements if used;
- Whistle blowing arrangements, including compliance with the Public Interest Disclosure Act;
- The procedures which staff should follow if a fraud is discovered;
- Guidance on training for the prevention and detection of fraud;
- Reference to the response plans that have been devised to deal with and minimize the damage caused by any fraudulent attack.

An example of a best practice fraud policy statement can be found at Appendix 10.

Fraud Response Plan

It is important that managers and others know what to do in the event of a fraud so that they can act without delay. It is recommended that departments prepare a fraud response plan. The objective of a fraud response plan is to ensure that timely and effective action can be taken.

The existence of a fraud response plan may, in itself, help to act as a deterrent as it shows that an organisation is prepared to defend itself against the risk of fraud. Appendix 11 provides more information about what to include in a best practice fraud response plan.

Promoting Staff Awareness of Fraud

All staff must be kept fully informed about the organisation's anti-fraud policy and what part they are expected to play in it. This can be achieved in a number of ways including providing every employee a copy of the organisation's ethics/anti-fraud policy as part of their contract of employment or staff handbook. Please see Appendix 9 for further detail.

Personnel Policies

Personnel recruitment policies play an important role in reducing the risk of fraud. Managers and staff responsible for staff recruitment must adhere strictly to the organisation's recruitment policy, particularly in relation to:

- The screening of references for new employees;
- Special arrangements for sensitive posts (e.g. checking police records);
- Detailed appraisal during probationary periods; and
- Detailed "exit" interviews for employees leaving the organisation.

8.1.2 Allocating Responsibilities for the Overall Management of Fraud Risk and for the Management of Specific Fraud Risks

It will be necessary to allocate responsibility for the overall management of fraud risk and for the management of anti-fraud activities. All those responsible for managing resources should be aware of the associated fraud risks. The ultimate responsibility and accountability for fraud risk rests with the Principal Accounting Officer although specific responsibility for managing the risk of fraud may be allocated to an appropriate senior officer. Where appropriate, the responsible officer should liaise with the Risk Management Committee and/or Audit Committee or equivalent where they have been set up in order to ensure that there is consistency in the scoring of fraud risk and in action taken to manage it. However, some fraud risks will require day to-day management and it will be important to assign responsibility for managing specific risks, once identified, at appropriate levels in the organisation. Establishing accountability and responsibility for specific fraud risks is necessary to:

- Encourage a culture of fraud risk awareness throughout the organisation;
- Ensure fraud risk remains well controlled; and

- Create a framework for the provision of reporting on the management of fraud risk to senior management.

Internal Audit

The role of internal audit is to deliver an opinion to the Principal Accounting Officer on the whole of an organisation's risk management, control and governance. In relation to fraud this will include the examination of the adequacy of arrangements for managing the risk of fraud and ensuring that the organisation actively promotes an anti-fraud culture.

Internal audit will therefore assist in the deterrence of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in the various segments of an organisation's operations. Internal audit's main responsibility is to ensure that management has reviewed its risk exposures and identified the possibility of fraud as a business risk.

Management has the responsibility for conducting fraud investigations but internal audit may be asked to assist, and in some organisations may have had responsibility for conducting investigations delegated to them. Fraud investigation is an area that requires specialist knowledge and where internal audit has this responsibility they need to develop and maintain appropriate levels of expertise.

Appendix 8 covers responsibilities for fraud risk ownership in more detail.

8.1.3 Establishing Cost Effective Internal Controls that are Commensurate with the Identified Risk

There are a range of controls (e.g. physical checks, reconciliation, supervisory checks, segregation and rotation of duties, and clear roles and responsibilities) that address risk, including that of fraud.

Departmental managers should consider which controls are most appropriate in their particular circumstances. In designing control, it is important that the control put in place is proportional to the identified risk. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Internal control can be classified in three ways:

- **Preventive controls**: those designed to limit the possibility of an undesirable outcome (e.g., a fraud) being realised. These are covered in Appendix 14.

- **Detective controls**: those established to identify errors, omissions and fraud after the events have taken place. Appendix 12 provides more information about detecting fraud.
- **Response controls**: those designed to ensure corrective action is taken and the harm caused by the fraudulent and corrupt activity is remedied. Appendix 11 provides more information about it.

Appendix 13 comprises a table of fraud indicators.

8.1.4 Developing the Right Skills and Expertise

This can be achieved by:

- Developing competency levels for both specialist anti-fraud personnel and more general operational staff, and
- Identifying a range of training courses/development events designed to enable staff to meet those competency levels. These can either be developed "in-house" or procured, and can include:
    - events on general subjects e.g. fraud identification, preventing fraud, IT crime, or
    - technical and specialist courses for key staff (e.g. managing a fraud incident, investigating a fraud, interviewing).

8.1.5 Responding Effectively to Fraud When it Occurs

Depending on the significance of the fraud, the fraud investigation process involves some or all of the following:

- Ensuring that the actions to take if fraud is discovered are clearly described in the organisation's Fraud Response Plan.
- Senior management providing the direction for any fraud investigation.
- Establishing clear terms of reference for the investigation.
- Appointing a Fraud Investigation Officer (FIO) to take charge of the investigation (usually a senior manager).
- Setting up a mechanism to report on progress of the investigation to appropriate senior levels of management.

- Controlling the investigation through procedures set out in the Fraud Response Plan.
- The overall investigation process involves:
    - Maintaining confidentiality;
    - Recovering assets;
    - Forensic investigations and protection of evidence;
    - Interviewing witnesses and dealing with employees under suspicion;
    - Controlling police involvement;
    - Managing civil proceedings;
    - Liaising with experts and regulators;
    - Preparing media statements; and
    - Reporting progress and findings to senior management.
- Ensuring that effective controls are in place to preserve all forms of evidence. This is a key factor if the fraudster is to be prosecuted successfully as evidence must be legally admissible in court.
- Deciding at an early stage the action to be taken with persons under suspicion and whether suspension or dismissal is necessary. Arrangements for interviewing suspects must be made and if criminal proceedings are initiated the Police must be involved. Paragraph 8(i) of Appendix 1 of the General Financial Rules states: 'As soon as a reasonable suspicion arises that a criminal offence has been committed, the senior officer of the department concerned present in the station will report to the Deputy Commissioner concerned and ask for a regular police investigation under the Code of Criminal Procedure, 1898, as adopted in Bangladesh'.
- Adhering to a "fair and reasonable" approach in interviews at all times.
- Setting up adequate measures to protect the business throughout the investigation process particularly when issuing statements to the media.
- Initiating a thorough review of all operating procedures in areas affected by the fraud.

Comprehensive reports presented to management should set out:

- Findings;
- Perceived weaknesses;

- Lessons learned; and
- Improvements required to reduce the risk of recurrence.

8.1.6 Establishing Appropriate Avenues for Reporting Fraud

There should be avenues for reporting suspicions of fraud. Staff should be encouraged to report suspicions of fraud either to their line mangers, to internal audit or possibly to a 'hotline' set up for the purpose. It is important that staff know where to report their suspicions and that any suspicions of fraud reported in this way are seen to be acted upon by management. Members of the public should also be encouraged to report their suspicions of fraud ensuring that avenues for reporting fraud are widely publicised and assuring whistle-blowers that any information received will be treated confidentially.

8.1.7 Continuously Monitoring the Risk Environment and Systems of Internal Control

The risk environment is constantly changing and priorities of objectives and the consequent importance of risks on the fraud risk profile will shift and change. Risk models have to be regularly revisited and reconsidered in order to have assurance that the fraud risk profile continues to be valid. The risk of fraud should also be considered along with other risks when major new policies are being developed, where a change in policy occurs or where changes are made to the way in which policy is to be implemented.

Control systems should be reviewed at regular intervals and in particular after restructuring, downsizing, changes in business processes, following identification of weaknesses, the introduction of new computer systems, and after an incident of fraud. It is also important to check that specific actions determined by management to reduce the risk of fraud are implemented as a matter of priority by the audited body. This is a role for internal audit.

8.1.8 Reporting Fraud Centrally

Audited bodies should report details of thefts and fraud within certain categories centrally annually (e.g., internal frauds, contractor frauds, some other frauds that contain useful lessons for a wider audience).

Audited bodies should be required to report details of any novel or unusual frauds centrally as soon as they become aware of them.

Paragraph 22 of the General Financial Rules states: 'With the exceptions noted below [regarding tax and petty losses], any loss of public money, departmental revenue or receipts, stamps, opium stores or other held by or on behalf of Government, caused by defalcation or otherwise, which is discovered in a treasury or other office or department, should be immediately reported by the officer concerned to his immediate official superior as well as to the Chief Accounts Officer concerned ... .such reports must be submitted as soon as a suspicion arises that there has been a loss ..... when the matter has been fully investigated, a further and complete report should be submitted of the nature and extent of the loss, showing the errors or neglect of rules by which such loss was rendered possible and the prospects of effecting a recovery'.

The centre should provide details of cases to other audited bodies so that they can be aware of the risks, and can take appropriate measures to reduce the risk of similar frauds being perpetrated against them.

The centre should also seek information concerning the means by which audited bodies develop their anti-fraud strategies. An annual questionnaire is issued to every central government organisation seeking answers to such questions as:

- Does the organisation have an anti-fraud policy?
- Is fraud risk regularly reviewed as part of the organisation's overall assessment of risk?
- Does the organisation have a fraud response plan?
- Does the organisation have a clearly established avenue for "whistle-blowers"?

The centre should use the information collected above to produce an annual Fraud Report that aims to inform departments of the scale and nature of certain categories of fraud, the circumstances in which these frauds occurred, the means by which they were recovered and the action taken against offenders. The information is provided to help departments learn from the experiences of others when reviewing and developing their own systems. The report also aims to increase awareness of fraud risk in specific areas and suggests ways in which the risk can be managed and reduced.

The Prevention of Money Laundering Act 2012 requires reporting organisations to report doubtful transactions in accordance with the terms of the Act. Reporting organisations are defined in section 2(w) of the Act.

8.2 Auditing the Response to Fraud Risk Assessment

A template has been designed to focus the audit on the two key components of fraud risk management: fraud risk assessment and fraud risk assessment response as shown in Appendix 3.

For each of the 8 key components of fraud risk assessment response an expected procedure has been identified:

1. There is a promotion of an anti-fraud culture by various means including (including a statement of ethical values, promotion of staff awareness of the risks of fraud and a policy on the recruitment of staff)
2. The ownership of fraud risks has been assigned to specific managers
3. Internal controls have been established to prevent and detect fraud
4. There is a training programme
5. There are procedures to respond to incidences of suspected fraud/fraud
6. Channels have been developed to record and report suspected fraud/fraud
7. There is a system for monitoring risk and internal controls including the implementation of remedial action
8. There are procedures for reporting fraud centrally.

The audit will comprise checking that the expected procedures have been adequately designed and implemented for the purposes of preventing and detecting fraud.

As detailed in ISSAI 4100 audit evidence may be gathered using a variety of techniques such as:

a) Observation
b) Inspection
c) Inquiry
d) Re-performance
e) Confirmation

Examples of test procedures have been included in the template – they are generic and may have to be adapted to the circumstances of a particular audited body.

The template also provides the facility to record a summary of the evidence obtained and a summary of key conclusions and recommendations.

As referred to in paragraph 93 of ISSAI 4100 the sufficiency of evidence relates to the quantity of the evidence. The competence, relevance, reliability and appropriateness of evidence relates to the quality of the evidence. Public sector auditors exercise professional judgement in making the determination of sufficiency and appropriateness throughout the evidence gathering process.

Sections 4-10 of the pilot audit report provided on page 39 cover the results of the auditing of the response to the fraud risk assessment of the audited body.

9. INTERNAL CONTROL CHECKLISTS FOR FRAUD PREVENTION AND DETECTION

9.1 Responsibility for Establishment of Internal Control System

The establishment of a good internal control system to prevent and detect fraud is primarily the responsibility of the executives and can help reduce the probability of fraud. Strong internal controls can help eliminate the elements that encourage fraud and prevent or deter fraud from occurring.

Some frauds are facilitated because of system weaknesses. Other frauds result from the failure to follow proper internal control procedures. Sometimes fraud occurs because too much trust has been placed in one individual with no effective separation of duties. When internal controls are not followed, or are ignored, or are overridden by management or others, the elements that enable fraud to occur emerge, and prime opportunities for fraudulent behavior exist.

Some fraud occurs because of the absence of a hands-on or supervisory review of transactions. For example, computer frauds, defined as those where the computer is instrumental in the perpetration of the fraud, sometimes result when transactions are processed that would ordinarily be questioned if they were processed manually and had been subject to a hands-on review.

While some individuals would never contemplate perpetrating a fraud, others may choose to engage in fraudulent actions if they think their fraudulent actions cannot be

prevented or will be undetected. A high probability of detection by internal controls that are designed to prevent or detect fraud will help deter the commission of fraud. However, fraud may still occur regardless of the strength of those internal controls.

Prevention of fraud is always preferable to the detection of fraud. Management must, therefore, develop a strong internal control system to prevent fraud. However, these preventive controls are almost never sufficient to stop those determined to attempt to carry out a fraudulent act or engage in fraudulent behavior. Therefore, detection controls are also important. Detection controls are established to detect fraud, errors, and omissions after these events have taken place, and if they have not been prevented.

9.2 Assessment of Internal Control System

Strong internal controls reduce the probability of fraud. Conversely weak controls increase the probability of fraud. Therefore, auditors must assess these controls so that they can identify weaknesses in them, or determine that appropriate controls do not exist at all. Weaknesses in internal controls may indicate to the auditor the real potential for fraudulent acts. Accordingly, the auditor should consider internal controls as important fraud deterrent and detection system components.

9.3 Internal Control Checklists

As a technique for detecting the absence of, or weaknesses in any of internal controls, it is a usual audit practice to develop an internal control checklist for each relevant area to be audited for use in assessing the adequacy of those internal controls. That checklist should be tailored to accommodate the audit environment. The results of the execution of each checklist by the auditor will provide him with information about the adequacy of the internal controls in each area, and contribute to the auditor's assessment regarding the potential for the existence of fraud.

Some model checklists with accompanying questions have been developed which may, however, be modified by the auditors while assessing the adequacy of internal controls in certain specific areas. These checklists are provided in the following sub-section.

9.3.1 Internal Control Checklist for Procurement Controls

Internal control checklist for assessing the adequacy of procurement controls may include the following questions:

Question Number	Check List Internal Controls – Procurement Controls	Yes	No
1	Is the delivery of materials checked to assure that they conform to contract or purchase order requirements for quality, quantity, and timely delivery?		
2	Have alternate sources of supply been developed or have purchases generally been made from single sources?		
3	Have contracts or purchase orders only awarded to the lowest responsible bidder?		
4	Are material changes to the contract or purchase order made after the award, subject to a documented review and approval process?		
5	Is a procedure in place to justify, document, and review the disqualification of contractors or vendors?		
6	Has a bid and proposal evaluation committee been established that evaluates bids and proposals using a documented bid /proposal evaluation process?		
7	Are procedures in place to prevent the release of procurement information to preferred or selected contractors or vendors?		
8	Is there a procedure in place to verify contractor or vendor certification as to the stage of contract completion or delivery?		
9	Are procedures in place to assure that all the bids and/or proposals received are valid and genuine?		
10	Have the controls ever detected fraud in this area?		

9.3.2 Internal Control Checklist for Physical Security Controls

Internal control checklist for assessing the adequacy of Physical Security controls may include the following questions:

Question Number	Check List Internal Controls – Physical Security	Yes	No
1	Are procedures in place that restricts access to accounting records to only authorized personnel?		
2	Are procedures in place that restricts access to information systems to only authorized personnel?		
3	Are inventory records maintained of all desktop computers and other computer equipment?		
4	Are periodic physical inventories taken of all desktop computers and computer equipment and other assets?		
5	Is the stock of blank checks used to pay suppliers, contractors, employees, and others kept in a secure, locked place?		
6	ls access to the stock of blank checks used to pay suppliers, contractors, employees, and others restricted to only authorize persons?		
7	ls access to the organization's premises controlled by a security force or, by other appropriate security measures?		
8	Are inventory records maintained of all furniture and office equipment?		
9	Have the controls ever detected fraud in this area?		

9.3.3 Internal Control Checklist for Organising Controls

Internal control checklist for assessing the adequacy of Organising controls may include the following questions:

Question Number	Check List Internal Controls – Organizing Controls	Yes	No
1	Has a table of organization been developed?		
2	Have the duties and responsibilities of all the positions on the table of organization been clearly defined and documented?		
3	Have position descriptions been prepared for all the positions on the table of organization?		
4	Are position descriptions subject to a periodic desk audit to determine whether the position descriptions reflect the duties actually being performed?		
5	Have the goals and objectives of the organization been clearly defined and documented?		
6	Have the levels of authority, including the use and application of resources, for all the positions on the table of organization been established, clearly articulated, and a documented?		
7	Have clear reporting lines been established and documented?		
8	Do the lines of reporting assure the most effective spans of control and provide for adequate supervision?		
9	Have any instances of fraud been detected by these controls?		

9.3.4 Internal Control Checklist for Supervision and Output Controls

Internal control checklist for assessing the adequacy of Supervision and Output controls may include the following questions:

Question Number	Check List Internal Controls – Supervision and Output Controls	Yes	No
1	Have guidelines been established for setting staff supervisor expectations?		
2	Have those guidelines been disseminated to all staff and all supervisors?		
3	Have procedures and standards been established to guide supervisory review?		
4	Are the results of supervisory reviews documented, filed and available for review?		
5	Are procedures in place to assure that supervisory reviews take place?		
6	Are procedures in place that provide for follow up or corrective action based on the supervisory review?		
7	Does the supervisory review process include random checks or unannounced checks or observations of staff output		
8	Does the supervisory review process include the examination of staff output and work products?		
9	Have any of the supervisory reviews uncovered fraud?		

9.3.5 Internal Control Checklist for Monitoring Controls

Internal control checklist for assessing the adequacy of Monitoring controls may include the following questions:

Question Number	Check List Internal Controls – Monitoring Controls	Yes	No
1	Has a performance measurement system been established to monitor the activities of each component of the organization?		
2	Do the performance measures include uniform, recognized measurement standards?		
3	Are these uniform, recognized standards periodically assessed to assure current applicability?		
4	Do the performance measures include assessments of efficiency?		
5	Do the performance measures include assessments of economy?		
6	Do the performance measures include assessments of effectiveness?		
7	Do the performance reviews include period-to-period comparisons of operational and financial data?		
8	Are deviations from performance standards documented and followed up to determine the reasons for the deviation?		
9	Have any of the performance measurement initiatives disclosed fraud?		

9.3.6 Internal Control Checklist for Evaluation Controls

Internal control checklist for assessing the adequacy of Evaluation controls may include the following questions:

Question Number	Check List Internal Controls – Evaluation Controls	Yes	No
1	Has an evaluation process been established to assure that the policies and procedures guiding each organizational component are periodically evaluated?		
2	Is the evaluation process being carried out as planned?		
3	Is a written report prepared after each evaluation documenting the results?		
4	Are the results of the evaluation process analyzed to determine Whet her corrective action is required?		
5	Are the reasons for the need for corrective action determined?		
6	Are corrective actions taken when warranted?		
7	Are the corrective actions taken analyzed to determine their effectiveness?		
8	Do independent evaluators perform the evaluations?		
9	Have any of the evaluations disclosed fraud?		

9.3.7 Internal Control Checklist for Staffing Controls

Internal control checklist for assessing the adequacy of Staffing controls may include the following questions:

Question Number	Check List Internal Controls – Staffing Controls	Yes	No
1	Are all positions supported by a documented position description?		
2	Are background checks and credential verifications performed of all potential employees before they are offered a position?		
3	Is all employment subject to a probationary period?		
4	Is the performance of all employees evaluated at least annually using a standard staff evaluation format?		
5	Are the employees who staff sensitive positions bonded or insured?		
6	Is provision made in staffing assignments for the separation of duties to prevent collusion?		
7	Is there a staff rotation policy in place for sensitive positions?		
8	Are spot checks and unannounced visits made to employee work Stations to monitor performance?		
9	Have any of the staffing controls detected fraud?		

9.3.8 Internal Control Checklist for Asset Accounting Controls

Internal control checklist for assessing the adequacy of Asset Accounting controls may include the following questions:

Question Number	Check List Internal Controls – Asset Accounting Controls	Yes	No
1	Is the asset register and the physical inventory periodically reconciled?		
2	Is there a written procedure in place to assure that all acquired assets are recorded promptly upon acquisition?		
3	Is there a procedure in place to assure that asset disposal is properly transacted and promptly recorded?		
4	Are all the assets subjected to a periodic review for obsolescence?		
5	Is the condition of all the assets subject to a periodic Inspection?		
6	Is a physical inventory taken each year of all assets?		
7	Are there policies and procedures in place to monitor the use of all assets?		
8	Are there controls in place to prevent the use of assets by employees and other unauthorized users?		
9	Is there a security system in place protecting all assets?		
10	Has fraud ever been detected by these controls?		

Appendices

Appendix 1

AUDIT PROGRAMME

Audit of audited body's procedures to prevent and detect fraud

Audited body: Date of audit:

Audit Steps	Manual ref	Checked by	W/P
PART 1: FRAUD RISK ASSESSMENT			
1. Overall Fraud Risk Assessment	7.1.1		
a. Design of procedure			
• Request a copy of the overall fraud risk assessment for inspection and assess the adequacy of design against the criteria listed in Appendix 4 to the manual.			
• Check that there is a requirement for fraud proofing of new policies, activities or operations to 'design out' fraud.			
b. Implementation			
• Check that the assessment is approved by senior management and used as a basis for fraud risk management and is regularly reviewed and updated.			
• Check any significant new polices, activities or operations for evidence of fraud proofing.			
2. Detailed Risk Assessment	7.1.2		
a. Design of procedure			
a) Request a copy of detailed risk assessments (or risk register) and check that they are designed to identify the processes or activities at risk and assess the nature and extent of the risks.			
b. Implementation			
b) Review the detailed risk assessments (or risk register) and check that they cover as appropriate			

Audit Steps	Manual ref	Checked by	W/P
the areas outlined in Appendices 5, 6 and 7 to the manual ('Identifying the processes or activities at risk to fraud', 'Assessing and ranking the nature and extent of vulnerability in each area' and 'Identifying particular forms of threat to each area' respectively).			
3. Evaluating the scale of fraud risks	7.1.3		
a. Design of procedure			
c) Review adequacy of design of procedures for evaluating the scale of fraud risks.			
b. Implementation			
d) Check the assessments made to check if they are reasonable and evidence based.			
PART 2: RESPONDING TO FRAUD RISK			
1 Promoting an anti-fraud culture	8.1.1		
a. Design of procedure			
e) Review adequacy of design of the promotion of an anti-fraud culture to check that it includes: (i) a statement of ethical values; (ii) anti-fraud policy (including coverage of promoting staff awareness of fraud); (iii) fraud response plan; (iv) HR policy regarding the recruitment of staff.			
b. Implementation			
f) Request copies of (i) statement of ethical values (ii) anti-fraud policy (iii) fraud response plan and (iv) HR policy regarding recruitment of staff and check that they are approved by senior management and distributed to all staff.			

Audit Steps	Manual ref	Checked by	W/P
2 Assigning specific responsibility for the ownership of fraud risks	8.1.2		
a. Design of procedure			
g) Check that there is a requirement for fraud risks to be allocated to specific managers and review the allocation procedures.			
b. Implementation			
h) Check that managers have been duly informed of their responsibilities and have acted upon them.			
3 Internal controls	8.1.3		
a. Design of procedure			
i) Check that preventative and detective internal controls have been adequately designed to prevent and detect fraud with reference to Appendix 13 of the manual (Risks and controls in specific systems)			
b. Implementation			
j) Check the operation of the controls identified once identified.			
4 Training	8.1.4		
a. Design of procedure			
k) Request a copy of the training strategy/programme for inspection and check it has been adequately designed to develop the right skills and expertise required to manage the risk of fraud effectively and to respond effectively to fraud when it occurs.			
b. Implementation			
l) Check that the key elements of the training strategy have been implemented as designed			
5 Responding to incidences of suspected fraud and fraud	8.1.5		
a. Design of procedure			

Audit Steps	Manual ref	Checked by	W/P
m) Check that procedures have to respond to incidences of suspected fraud and fraud have been designed to cover: • that the actions to take if fraud is discovered are clearly described in the Organisation's Fraud Response Plan; • senior management providing the direction for any fraud investigation; • establishing clear terms of reference for the investigation; • appointing a Fraud Investigation Officer (FIO) to take charge of the investigation (usually a senior manager); • setting up a mechanism to report on progress of the investigation to appropriate senior levels of management; • controlling the investigation through procedures set out in the Fraud Response Plan (as per Appendix 9 to the manual); • ensuring that effective controls are in place to preserve all forms of evidence. This is a key factor if the fraudster is to be prosecuted successfully as evidence must be legally admissible in court; • deciding at an early stage the action to be taken with persons under suspicion and whether suspension or dismissal is necessary. Arrangements for interviewing suspects must be made and if criminal proceedings are initiated the Police must be involved; • adhering to a "fair and reasonable" approach in interviews at all times;			

Audit Steps	Manual ref	Checked by	W/P
• setting up adequate measures to protect the business throughout the investigation process particularly when issuing statements to the media; • initiating a thorough review of all operating procedures in areas affected by the fraud; • issuing comprehensive reports to management which set out: ▪ findings; ▪ perceived weaknesses; ▪ lessons learned; and ▪ Improvements required reducing the risk of recurrence.			
b. Implementation			
(n) For a sample of frauds and suspected fraud investigations check that the procedures have been followed as appropriate.			
6 Reporting fraud	8.1.6		
a. Design of procedure			
Request a copy of the audited body's procedures for reporting suspected fraud/fraud and check that they are adequately designed. The procedures ought to include: (i) arrangements to safeguard the confidentiality of the information provided; (ii) the promotion of the awareness of reporting concerns procedures; (iii) procedures for assessing and referring the information provided; (iv) management training; (v) the provision of a channel for reporting			

Audit Steps	Manual ref	Checked by	W/P
concerns independent of the audited body.			
b Implementation			
• Check that the audited body's procedures for reporting fraud are approved by senior management and widely distributed and implemented as designed.			
7 Monitoring risk and the effectiveness of internal control	8.1.7		
a Design of procedure			
• Check the adequacy of the audited body's procedures designed to monitor risk and internal controls including the implementation of any remedial action necessary.			
b. Implementation			
• Check that the audited body's procedures for monitoring monitor risk and internal controls including the carrying out of any remedial action necessary have been implemented.			
8 Reporting fraud centrally	8.1.8		
a. Design of procedure			
Check the adequacy of procedures designed to report details of thefts and frauds centrally. Check that the procedures include requirements to: (i) reporting fraud centrally annually and any novel or unusual frauds as soon as they occur (ii) analysing reported fraud and informing audited bodies of fraud risk in specific areas and suggesting ways in which the risk may be managed and reduced.			
b. Implementation			
• Check that the procedures to report fraud have been adequately implemented.			

Appendix 2

MODEL OF AUDIT FINDINGS, AND DEVELOPING AUDIT PARAGRAPH ON FRAUD AUDIT

(Reference- pilot audit report of Local and Revenue Audit Directorate conducted by SPEMP-B Project)

Background

The Local & Revenue Audit Directorate of the CAG of Bangladesh conducted a review of fraud prevention procedures and undertook a forensic investigation with the assistance of the Strengthening Public Expenditure Management Programme (SPEMP-B) project. The pilot audit team was supported by a national and an international expert.

This report presents the findings and recommendations arising from our examination of fraud prevention procedures. In line with best practice a separate report will be issued covering our forensic investigation.

Our examination involved assessing the fraud prevention procedures in place against a set of expected or model procedures using the guidance in the Office of the Comptroller and Auditor General (OCAG) Fraud Audit Manual. We used a self-assessment checklist and held a meeting to discuss the responses.

Paragraph 28 of the OCAG Audit Code requires that 'Auditors should establish whether audited bodies have taken reasonable steps in relation to the limitation of the possibility of fraud ...'.

There are two key components to fraud prevention (or fraud risk management) which are fraud risk assessment and fraud risk response.

Our examination covered the following ten key fraud risk assessment and fraud risk response areas:

(i) Overall fraud risk assessment including fraud-proofing;
(ii) Detailed fraud risk assessment identifying and assessing the areas most vulnerable to fraud;
(iii) Evaluating of the significance of fraud risks;
(iv) Promoting an anti-fraud culture;
(v) Assigning specific responsibility for the ownership of fraud risks;
(vi) Establishing internal controls to prevent and detect fraud;
(vii) Responding to incidences of suspected fraud and fraud;

(viii) Whistle blowing procedures to record and report suspected fraud and fraud;

(ix) Monitoring fraud risk and internal controls including the implementation of remedial action;

(x) Reporting fraud centrally.

We have set out our observations and recommendations below. We would be very grateful for management responses within the normal four week period and we would like to arrange a meeting to discuss the responses provided.

Our key recommendations concern the fraud risk register, internal controls and a fraud response plan.

Findings and recommendations

1. OVERALL FRAUD RISK ASSESSMENT

There is no documented overall assessment of fraud risk or a methodology currently in place to systematically assess fraud risk.

Comment:

An overall fraud risk assessment involves assessing the organisation's overall vulnerability to fraud. Where the risk of fraud is considered to be low a specific fraud risk assessment may not be necessary with any risks being considered instead as part of the organisation's overall risk assessment. However, it will still be necessary for those organisations to develop an anti-fraud culture.

Fraud proofing is a useful and pre-emptive way of making a risk assessment of new systems. Teams may be set up and used to play the role of fraudsters to simulate fraud and to identify weaknesses – a little like 'war games'.

Recommendation:

We recommend that an overall fraud risk assessment is carried out and documented.

Management response-

2. IDENTIFYING AND ASSESSING THE AREAS MOST VULNERABLE TO FRAUD

Finding:

There is no documented assessment of the areas most vulnerable to fraud.

Comment:

The more detailed assessment of fraud risk will identify the areas in which an organisation may face fraud threats and the types of threat it may face. It involves identifying the processes or activities at risk of fraud within the organisation. Using a fraud risk register is a very effective way to facilitate it.

A fraud risk register is a register or listing of fraud risks, fraud risk assessments and responses. It is a key procedural tool in preventing fraud and very importantly facilitates a 'resources to risk' approach which provides for the allocation of scarce resources to address the areas of highest fraud risk.

Further guidance on fraud risk registers is provided at Annex A.

Recommendation:

We recommend that a fraud risk register is set up and maintained to identify and assess the areas most vulnerable to fraud.

Management response:

3. EVALUATING THE SIGNIFICANCE OF FRAUD RISKS

Finding:

There is no documented assessment of the significance of fraud risks.

Comment:

In deciding how to handle fraud risks it is important to evaluate their significance. The evaluation ought to include an assessment of the strength of mitigating internal controls. It ought to assess the likelihood and impact of fraud. Furthermore, the assessment of the impact of the risk should not simply take account of the financial impact but should also consider the organisation's reputation. A qualitative approach usually involves grading risks as low, medium or high.

Recommendation:

We recommend that an assessment of the significance of fraud risks is carried out and documented based on an assessment of the likelihood and impact using a fraud risk register.

Management response:

4. PROMOTING AN ANTI-FRAUD CULTURE

Finding:

The organisation has a statement of ethical values and seeks to promote staff awareness of fraud risks.

Comment:

Promoting an anti-fraud culture is of fundamental importance to the prevention of fraud. It is founded on a documented anti-fraud policy. The policy ought to cover, among other things, the responsibilities for managing fraud risks and the resources available to do so and the methods of promoting an anti-fraud culture including the use of circulars, posters, job descriptions and training courses.

An anti-fraud policy statement should be circulated to all stakeholders which is simple, focused and easily understood. It should refer to a zero tolerance policy to fraud and avenues for reporting suspected fraud.

Recommendation:

We recommend that an anti-fraud policy and an anti-fraud policy statement are drawn up and used to promote an anti-fraud culture.

Management response:

5. ASSIGNING SPECIFIC RESPONSIBILITY FOR THE OWNERSHIP OF FRAUD RISKS

Finding:

The ownership of fraud risks is implied rather than explicit.

Comment:

The ultimate responsibility and accountability for fraud risk rests with the Director although specific responsibility for managing the risk of fraud may be allocated to an appropriate senior officer. However, many fraud risks will require day to-day management and it will be important to assign responsibility for managing specific risks, once identified, at appropriate levels in the organisation. Establishing accountability and responsibility for specific fraud risks is necessary to:

- encourage a culture of fraud risk awareness throughout the organisation;
- ensure fraud risk is well controlled; and
- create a framework for the provision of reporting on the management of fraud risk to senior management.

Recommendation:

We recommend explicit responsibility for the ownership of fraud risks is assigned to appropriate members of staff in the organisation. A fraud risk register would provide a very suitable vehicle to do this.

Management response-

6. ESTABLISHING INTERNAL CONTROLS TO PREVENT AND DETECT FRAUD

Finding:

Internal controls have not been implemented to prevent and detect fraud in the areas of procurement/purchasing and storekeeping.

Internal controls are set out in the PPR and Internal Controls manuals. It is generally understood that if the rules are followed the risk of fraud is greatly reduced. However, our forensic investigations audit has revealed that the controls are not effectively implemented.

Comment:

There are a range of internal controls (e.g., physical checks, reconciliation, supervisory checks, segregation and rotation of duties and clear roles and responsibilities) that address risk including that of fraud.

Managers should consider which controls are most appropriate in their particular circumstances. In designing control, it is important that the controls put in place are proportional to the risks identified. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Internal control can be classified in three ways:

- **preventive controls:** those designed to limit the possibility of an undesirable outcome such as a fraud being realised;
- **detective controls:** those established to spot errors, omissions and fraud after the events have taken place.
- **Response controls**: those designed to ensure corrective action is taken and the harm caused by the fraudulent and corrupt activity is remedied.

Management response:

Recommendation:

We recommend that internal controls are established and implemented to prevent and detect fraud. We attach a copy of OCAG Fraud manual guidance regarding internal controls for your assistance at Appendix-14 and we would be happy to provide further advice as required.

7. RESPONDING TO INCIDENCES OF SUSPECTED FRAUD AND FRAUD

Finding:

The Contract handbook provides general guidance on responding to suspected fraud and fraud. However, there is no specific guidance on how to respond to incidences of suspected fraud and fraud.

Comment:

A detailed fraud response plan should cover the following areas as a minimum:

- instructions on the action required at the point of discovery;

- to whom the fraud or suspicion of fraud should be reported in the first instance;
- how the fraud should be investigated and who will lead the investigation;
- how to secure evidence without alerting suspects at the outset of the investigation;
- how to secure the evidence in a legally admissible form;
- guidance about dealing with employees under suspicion (with reference to the procedures included in the Financial Rules, Disciplinary Rules for Govt. Employees and the Departmental manuals);
- guidance about interviewing (decisions about interviewing suspects must be made by senior management);
- when and how to contact the police. Any decision about involving the police must be taken by senior management;
- guidance about recovering assets (e.g., action to trace and freeze assets; action to prevent the release of assets; obtaining search orders);
- what experts to contact for advice;
- how to mitigate the threat of future fraud by taking appropriate action to improve controls;
- how to disseminate the lessons learned from the experience in cases where there may be implications for the organisation as a whole.

Recommendation:

We recommend that specific guidance is drawn up in the form of a detailed fraud response plan covering the areas outlined above.

Management response:

8. WHISTLEBLOWING PROCEDURES TO RECORD AND REPORT SUSPECTED FRAUD AND FRAUD

Finding:

There are no documented whistle blowing procedures although there is a strong expectation that staff will report suspected fraud and fraud.

Comment:

There should be very clearly defined avenues for reporting suspicions of fraud. Staff should be encouraged to report suspicions of fraud either to their line mangers or to internal audit or to a dedicated 'hotline' set up for the purpose. It is important that staff know where to report their suspicions and that any suspicions of fraud reported in this way are seen to be acted upon by management. Members of the public should also be encouraged to report their suspicions of fraud ensuring that avenues for reporting fraud are widely publicised and assuring whistleblowers that any information received will be treated confidentially.

Recommendation:

We recommend that specific whistle blowing guidance is drawn up based on up to date best practice followed by other nations.

Management response:

9. MONITORING FRAUD RISK AND INTERNAL CONTROLS INCLUDING THE IMPLEMENTATION OF REMEDIAL ACTION

Finding:

There is no system for monitoring fraud risk and internal controls including the implementation of remedial action.

Comment:

The risk environment is constantly changing and priorities of objectives and the consequent importance of risks on the fraud risk profile will shift and change. Risk models have to be regularly revisited and reconsidered in order to have assurance that the fraud risk profile continues to be valid. The risk of fraud should also be considered

along with other risks when major new policies are being developed, where a change in policy occurs or where changes are made to the way in which policy is to be implemented.

Control systems should be reviewed at regular intervals and in particular after restructuring, downsizing, changes in business processes, following identification of weaknesses, the introduction of new computer systems and after an incident of fraud. It is also important to check that specific actions determined by management to reduce the risk of fraud are implemented as a matter of priority by the audited body.

Recommendation:

We recommend that a system for monitoring fraud risk and internal controls including the implementation of remedial action is introduced. A risk register is a very suitable vehicle for this purpose.

Management response:

10. REPORTING FRAUD CENTRALLY

Finding:

Depending on individual merit reporting is carried out up to an appropriate level.

Comment:

Reporting to the Ministry of Finance would enable the Ministry to forewarn and thereby forearm other government bodies against similar types of fraud.

Recommendation:

We recommend that reporting fraud centrally to the Ministry of Finance is carried out as a matter of routine.

Management response:

Appendix 3

TEMPLATE OF PROCEDURES FOR A REVIEW OF AN AUDITED ENTITY'S PROCEDURES TO PREVENT AND DETECT FRAUD

PART 1: FRAUD RISK ASSESSMENT

Sl.No.	Component	Background	Expected procedure in the audited body	Manual reference	Procedure adequately designed?	Summary of evidence	Procedure implemented?	Summary of evidence	Conclusions and recommendations
1	**OVERALL FRAUD RISK ASSESSMENT** Assessing the Organisations overall Vulnerability to Fraud	Vulnerability to fraud can be assessed at different levels in an organization. A [quick/ general] assessment of the overall level of risk an organisation is exposed to is often a good starting point. A fraud risk assessment should additionally be carried out during the development of any new policies, activities or operations to ascertain whether any new risks arise that need to be managed.	There is an overall assessment of fraud risk During the development of new policies, activities or operations fraud risk assessments are carried out for fraud proofing purposes.	7.1.1 7.1.1	Test: Request a copy of the overall fraud risk assessment for inspection and assess the adequacy of design against the criteria listed in Appendix 4. Test: Check that there is a requirement for fraud proofing of new policies, activities or operations to 'design out' fraud.		Test: Check that the assessment is approved by senior management and used as a basis for fraud risk management and is regularly reviewed and updated. Test: Check any significant new polices, activities or operations for evidence of fraud proofing.		
2	**DETAILED FRAUD RISK ASSESSMENT** Identifying the Areas most Vulnerable to	This more detailed assessment of fraud risk will result in an "exposure profile" or fraud risk framework	The areas most vulnerable to fraud have been identified and assessed	7.1.2	Test: Request a copy of detailed risk assessments (or risk register) and check that they are designed to identify the processes or		Test: Review the detailed risk assessments (or risk register) and check that they cover as appropriate the areas outlined in		

Sl.No.	Component	Background	Expected procedure in the audited body	Manual reference	Procedure adequately designed?	Summary of evidence	Procedure implemented?	Summary of evidence	Conclusions and recommendations
	Fraud	that identifies the areas in which an organisation may face fraud threats and the types of threat it may face. The steps in this stage include: ● Identifying the processes or activities at risk of fraud. ● Assessing and ranking the nature and extent of vulnerability in each area. ● Identifying the particular forms of fraud threat to each area.			activities at risk and assess the nature and extent of the risks.		Appendices 5, 6 and 7. 5 = Identifying the processes or activities at risk to fraud. 6 = Assessing and ranking the nature and extent of vulnerability in each area. 7= Identifying particular Forms of Threat to Each Area		
3	Evaluating the scale of fraud risks	In deciding how to handle the fraud risks identified it is important to evaluate their significance. An analysis of threats against compensating factors such as internal controls is a key part of this task. Management should agree on the most appropriate definition and number of categories to be	The scale of fraud risks has been assessed taking into account the strength of internal controls.	7.1.3	Test: Review adequacy of design of procedures for evaluating the scale of fraud risks		Test: Check the assessments made to check if they are reasonable and evidence based.		

Sl.No.	Component	Background	Expected procedure in the audited body	Manual reference	Procedure adequately designed?	Summary of evidence	Procedure implemented?	Summary of evidence	Conclusions and recommendations
		used when assessing both the likelihood and impact of each risk. The assessment of the impact of the risk should not simply take account of the financial but should also consider the organisation's reputation, and recognise the potential political and commercial sensitivities involved. A qualitative approach usually involves grading risks in HIGH, MEDIUM or LOW categories.							
PART 2: RESPONDING TO FRAUD RISK									
1	Promoting an anti-fraud culture Developing and Promoting an anti-fraud culture.	Having a clear statement of ethical values; • Establishing a clear anti-fraud policy and fraud response plan; • Promoting staff awareness of fraud; • Recruiting honest staff (checking references etc.); • Maintaining good staff morale.	There is a promotion of an anti-fraud culture by various means	8.1.1 and Appendices 9, 10 and 11 (9 = anti-fraud culture 10= anti-fraud policy 11= Fraud Response Plan)	Test: Review adequacy of design of the promotion of an anti-fraud culture to check that it includes: (i) a statement of ethical values (ii) anti-fraud policy (including coverage of promoting staff awareness of fraud) (iii) fraud response plan (iv) HR policy regarding the		Test: Request copies of (i) statement of ethical values (ii) anti-fraud policy (iii) fraud response plan and (iv) HR policy regarding recruitment of staff and check that they are approved by senior management and distributed to all staff.		

Sl.No.	Component	Background	Expected procedure in the audited body	Manual reference	Procedure adequately designed?	Summary of evidence	Procedure implemented?	Summary of evidence	Conclusions and recommendations
					recruitment of staff.				
2	**ASSIGNING OWNERSHIP** Assigning specific responsibility for the ownership of fraud risks	The ultimate responsibility and accountability for fraud risk rests with the Accounting Officer although specific responsibility for managing the risk of fraud may be allocated to an appropriate senior officer such as the PFO. However, some fraud risks will require day to-day management and it will be important to assign responsibility for managing specific risks.	The ownership of fraud risks has been assigned to specific managers	8.1.2 and Appendix 8	Test: Check that there is a requirement for fraud risks to be allocated to specific managers and review the allocation procedures.		Test: Check that managers have been duly informed of their responsibilities.		
3	**ESTABLISHING INTERNAL CONTROL** Establishing cost effective internal controls to detect and deter fraud which are commensurate with the identified risk	Internal controls comprise: ● Preventive controls: those designed to limit the possibility of an undesirable outcome (e.g. a fraud) being realised. ● Detective controls: those established to spot errors, omissions and fraud after the events have taken place.	Internal controls have been established	8.1.3 and Appendices 12 13, 14 and 15 (12 = detecting fraud 13= Fraud indicators 14= Reducing opportunities for fraud 15= Risks and controls in specific systems)	Test: Check that preventative and detective internal controls have been adequately designed to prevent and detect fraud with reference to 7-8 and 5-6 respectively.		Test: Check the operation of the controls identified once identified.		

Sl.No.	Component	Background	Expected procedure in the audited body	Manual reference	Procedure adequately designed?	Summary of evidence	Procedure implemented?	Summary of evidence	Conclusions and recommendations
					"fair and reasonable" approach in interviews at all times (x) Setting up adequate measures to protect the business throughout the investigation process particularly when issuing statements to the media (xi) Initiating a thorough review of all operating procedures in areas affected by the fraud. Comprehensive reports presented to management should set out: ● Findings; ● Perceived weaknesses; ● Lessons learned; and ● Improvements required to reduce the risk of recurrence.				
6	REPORTING FRAUD Establishing appropriate channels for reporting fraud	There should be system of reporting for suspicions of fraud. Staff should be encouraged to report suspicions of fraud either to their line mangers, to internal audit or possibly to a hotline set up for the purpose. It is important that staff know where to report their suspicions and that any	Channels have been developed to record and report suspected fraud/fraud	8.1.6	Test: Request a copy of the audited body's procedures for reporting suspected fraud/fraud and check that they are adequately designed. The procedures ought to include: (i) arrangements to safeguard the confidentiality of the information provided, (ii) the promotion		Test: Check that the audited body's procedures for reporting fraud are approved by senior management and widely distributed and implemented as designed.		

Sl.No.	Component	Background	Expected procedure in the audited body	Manual reference	Procedure adequately designed?	Summary of evidence	Procedure implemented?	Summary of evidence	Conclusions and recommendations
		suspicions of fraud reported in this way are seen to be acted upon by management. Members of the public should also be encouraged to report their suspicions of fraud through advertising campaigns, offering rewards, ensuring that avenues for reporting fraud are widely publicised and assuring whistle-blowers that any information received will be treated confidentially.			of the awareness of reporting concerns procedures (iii) procedures for assessing and referring the information provided (iv) management training (vi) the provision of a channel for reporting concerns independent of the audited body.				
7	MONITORING RISK AND THE EFFECTIVENESS OF INTERNAL CONTROL Monitoring the implementation of specific actions determined by management to reduce the risk of fraud	A system is required to monitor and follow up implementation of specific actions determined by management. A detailed timetable should be established for each item requiring action and regular progress reports produced for senior management review. It is essential to monitor this timetable through the Risk Committee, where an	There should be a system for monitoring risk and internal controls including the implementation of any remedial action necessary.	8.1.7	Test: Check the adequacy of the audited body's procedures designed to monitor risk and internal controls including the implementation of any remedial action necessary.		Test: Check that the audited body's procedures for monitoring monitor risk and internal controls including the carrying out of any remedial action necessary have been implemented.		

Sl.No.	Component	Background	Expected procedure in the audited body	Manual reference	Procedure adequately designed?	Summary of evidence	Procedure implemented?	Summary of evidence	Conclusions and recommendations
		organisation has such a body, through the Audit Committee when there is no separate Risk Committee or for somebody to monitor and report to senior management.							
8	**REPORTING FRAUD CENTRALLY** Audited bodies should report details of thefts and fraud within certain categories centrally annually.	Reporting fraud centrally allows the information collected to be used to inform audited bodies of the scale and nature of certain categories of fraud, the circumstances in which these frauds occurred, the means by which they were recovered and the action taken against offenders. The information is provided to help departments learn from the experiences of others when reviewing and developing their own systems. The report also aims to increase awareness of fraud risk in specific areas and suggests ways in which the risk can be managed and reduced.	There should be procedures for reporting fraud centrally annually and for reporting any novel or unusual frauds as soon as they become aware of them.	8.1.8	Test: Check the adequacy of procedures designed to report details of thefts and frauds centrally. Check that the procedures include requirements to: (i) reporting fraud centrally annually and any novel or unusual frauds as soon as they occur (ii) analysing reported fraud and informing audited bodies of fraud risk in specific areas and suggesting ways in which the risk may be managed and reduced.		Test: Check that the procedures to report fraud have been adequately implemented.		

Appendix 4

CHECKLIST FOR ASSESSING OVERALL FRAUD RISK

- Does the organisation view fraud within the context of wider risks (e.g. the risk of errors and irregularities)?
- Is there a definition of the processes or activities open to fraud? It is fundamental to fraud risk assessment to know the scope of the problem the organisation is managing.
- If the risk of fraud is considered to be high is there a fraud risk assessment including a comprehensive risk log? The fraud risk assessment should include, as a minimum, a basic register or log that identifies the risks. It should include a separate assessment of both the impact and the likelihood of each risk and should be a living document that is continuously updated to reflect changing circumstances.
- Does the organisation have effective recruitment procedures to reduce the risk of employing potential fraudsters?
- How does the organisation demonstrate zero tolerance to fraud? Government bodies should have a policy demonstrating to all those that might seek to defraud the Government that such action is not acceptable and will not be tolerated. This can take many forms such as wording on claim forms and declarations, advertising campaigns, statements on websites, and publicity about sanctions including prosecutions. All staff and external contractors should be aware of the organisation's attitude to fraud and their consequences.
- Is there a clear statement of commitment to ethical business behaviour throughout the organisation to help ensure that staff know that they are expected to follow the rules without circumventing controls and that they should avoid or declare any conflicts of interest?
- Does the organisation have a fraud policy statement to communicate the organisation's approach to fraud? Such a statement may include some or all of the following areas:
    - Allocation of responsibilities for the overall management of fraud;
    - The procedures which staff should follow if fraud is discovered;

- Guidance on training for the prevention and detection of fraud;
- Reference to response plans that have been devised to deal with and minimise the damage caused by fraudulent attack.

- Does the organisation have a fraud response plan? It is important that managers know what to do in the event of fraud so that they can act without delay. An effective fraud response plan should be closely tailored to each organisation's circumstances and should reflect the likely nature and scale of losses. A fraud response plan should cover:
  - To whom the fraud or suspicion of fraud should be reported in the first instance (e.g. senior managers' personnel or internal audit);
  - How the organisation should investigate fraud;
  - How to secure evidence in a legally admissible form;
  - When and how to contact the police;
  - How to initiate recovery action;
  - Who else to contact for advice (e.g. insurers, regulatory bodies, legal advisers, parent department, press office);
  - How to disseminate the lessons learned from fraud cases.
- Does the organisation have an effective fraud awareness programme?
- Does the organisation have clear reporting channels for reporting suspicions of fraud that offer protection to those reporting fraud? Suitable avenues can include line management, senior management, a specialist fraud team or internal audit. Organisations can also establish fraud hotlines so that staff can report suspicions of fraud confidentially. It is important that all cases of reported fraud or suspicions of fraud are acted upon.
- Does the organisation have an effective framework for reporting details of fraud and thefts centrally?

Appendix 5

IDENTIFYING THE PROCESSES OR ACTIVITIES AT RISK TO FRAUD

The starting point is to identify the organisation's major activity areas in terms of:

- Product and service outputs and deliverables;
- Operational areas and locations;
- Revenue generation;
- Revenue collection;
- Expenditure;
- Suppliers and inputs;
- Asset utilisation, acquisition and disposal;
- Customer/client records.

Appendix 6

ASSESSING AND RANKING THE NATURE AND EXTENT OF VULNERABILITY IN EACH AREA

A rating should be given to each of the areas identified in the previous step in terms of its potential vulnerability to both internal and external fraud. All areas should be ranked by their vulnerability factor and listed from the highest down to the lowest. Some common criteria/factors used to make judgements about vulnerability include:

- Materiality;
- Economic indicators;
- Fraud history;
- Last time the activity/function was reviewed;
- Concerns of management;
- Staff attitudes and values;
- Management attitudes and values;
- Quality of management;
- Internal control history for the area;
- Extent of effective reporting mechanisms;
- Internal and external audit risk assessment ratings for the area;
- Degree of operational complexity;
- Overall size, scope and value of activities;
- Impact of technology;
- Organisational culture.

Appendix 7

IDENTIFYING THE PARTICULAR FORMS OF FRAUD THREAT TO EACH AREA

1. Each area can be assessed in terms of particular forms of threat such as:

    - Theft;
    - Misappropriation of funds or assets;
    - Fraudulent administration of contracts;
    - Falsification of source records for improper advantage.

2. Recognising Red Flags

There are many general fraud symptoms and indicators, called "Red Flags", those auditors must be alert for. These include:

a. Poor internal controls,
b. Management override of internal controls,
c. Missing documentation,
d. Inappropriate and incorrect bookkeeping and poorly maintained accounting Records,
e. Active or passive resistance to audit inquiries such as denying or delaying auditor access to records or to personnel,
f. Shortages and overages in cash,
g. Shortages and numerous adjustments to inventories.

In addition there are also very recognizable, very specific Red Flags or fraud indicators that exist in specific activities that may indicate to the auditor the possible presence of fraud. For example:

I. Procurement and Contracting

Crores of Taka are expended annually to purchase goods and services, and on capital improvements and construction. Because of the financial enormity of these expenditures, and the widely documented propensity for fraud in this area, it is

essential that auditors recognize the indicators of fraud in procurement and contracting activities.

I.I Common Procurement and Contracting Fraud indicators

a. Procurement of services, goods, or work projects not needed, or in excess of what may be required.
b. Needs assessments for services, goods, or work projects that are not adequate or are not accurately developed.
c. Requirements that justify continuing to contract with or buy from only certain contractors or vendors.
d. Defining requirements so that only certain contractors or vendors can supply them.
e. Unsuccessful bidders who become subcontractors, or goods and services suppliers.
f. Contracting or purchasing from a single source without developing alternate sources of goods and services.
g. Work statements or material specifications that appear to fit a favoured or single contractor or vendor.
h. Releasing procurement information to preferred or selected contractors or vendors.
i. Consulting with preferred contractors and vendors about requirements and specifications.
j. Designing pre-qualification standards, specifications or conditions to limit competition to preferred vendors or contractors.
k. Splitting contract requirements to so that contractors and vendors can share or rotate bids and awards.
l. Splitting procurement requirements to avoid procurement policies.
m. Lost or misplaced vendor or contractor bid proposals and price quotations.
n. Questionable disqualification of a contractor or vendor.
o. Biased proposal evaluation criteria.

p. Award of contract or purchase order to other than lowest responsible bidder.

q. Material changes to the contract or purchase order after the award.

r. Awards to contractors or vendors with a history of poor or questionable performance.

s. Incorrect certification by the contractor or vendor as to the stage of contract completion or delivery of goods and services.

t. The delivery of services or materials that do not conform to contract or purchase order requirements.

u. Acceptance without verification of contractor or vendor certification of service and material quality.

II. Treasury/Cash Functions

Cash is the focal point of most entities. Virtually every transaction involves the transfer of cash into or out of an organization. In that regard and because of its liquid nature, cash transactions pose significant inherent risk and are highly susceptible to fraud. There are many ways to misappropriate cash.

II.I Common Petty Cash Fraud Indicators

a. Shortages/overages in petty cash funds.

b. Forged, fictitious or unusual vouchers in the petty cash box.

c. Numerous, receipts for hard to verify expenditures, like postage, and office supplies.

d. Borrowing from petty cash supported by promissory notes.

e. Cash advances.

f. Lack of approval for petty cash disbursements.

g. Dummy or altered receipts.

II.II Common Cash from Bank Account Fraud indicators

a. Ghosts on payroll.

b. Missing paid checks.
c. Checks payable to employees.
d. Endorsements on checks that do not match other writing samples.
e. Checks that have a second endorsement.
f. Void checks.
g. Cash collections not deposited in the bank.
h. Conducting cash sales and failing to record the sales.
i. Collecting a cash sale and recording only a part of the sale.
j. Lapping and kiting.
k. Receiving cash and only crediting an account for a part of the sale.
l. Receiving/ recording cash, not depositing it, and calling it deposit in Transit.
m. Removing money from a cash bank deposit and not explaining the shortage.

III. Assets/Inventory

Assets/inventory are very common targets of fraud. Assets/inventory have value, can be sold or converted to cash, are useful even if not sold, and often are not adequately protected.

III.I Common Assets and inventory Fraud indicators

a. Personal items purchased and charged to an asset or inventory account.
b. Disbursement schemes charged to assets or inventory, such as other fictitious costs paid or stolen by an employee.
c. Vendor fraud in which the customer purchases assets or inventory from a vendor and the vendor diverts the shipment to another customer, to the employee, or kicks-back money to an employee.
d. Manipulating asset and inventory counts and inventory and asset valuations.
e. Inflating the data on actual thefts and shortages to cover in-house thefts.
f. Inflating asset or inventory prices.
g. Arranged cooperative thefts with inside/outside personnel.
h. Overstating asset or inventory counts in number and value by manipulating counts and values.
i. Declaring assets or inventory obsolete that is not obsolete, selling it, disposing of it, or converting it for one's own use.

j. Failing to write-down, or delete from inventory obsolete asset or inventory items after declaring them obsolete so they continue to be counted.
k. Stealing assets or inventory by placing them in a trash container.
l. Purchasing outdated or already-obsolete assets or inventory.
m. Mismarking sealed containers and boxes in storage or inventory as to quantity, quality.

III.II Pension And investment Fund Operations

Frauds in the management and administration of pension and investment funds may occur in two basic ways:

a. Poor investments tied to self-dealing or commercial bribery.
b. Embezzlement or the conversion to one's own use or benefit the money or property of another, over which one exerts a fiduciary control.

Trustees, fund employees, employers and outsiders, may all commit this type of fraud.

III.III Common Pension and Investment Fund Fraud Indicators

Embezzlement or the conversion to one's own use or benefit the money or property of another, over which one exerts a fiduciary control, is often evidenced by:

a. Inadequate, incomplete, inaccurate records of, and support for transactions.
b. The use, sale, compromise of insider and confidential information.
c. Less than prompt communications to oversight committees, and trustees.
d. Benefits paid to dead or otherwise ineligible beneficiaries.
e. Unusual number of changes made to beneficiary records, including changes in addresses, amounts, and benefit computations.
f. Signatures on benefits checks that do not match other signature samples.
g. Multiple and unapproved changes to beneficiaries' survivor authorizations.
h. Errors in computations made to beneficiary accounts.
i. Complaints by beneficiaries about payments, including late payments, incorrect payments, and payments not received.
j. Failure to reconcile balances in control accounts.

Poor investments tied to self-dealing or commercial bribery are sometimes evidenced by:

a. Pension or investment fund personnel maintaining less than arms' length relationships with outside investment advisors and security representatives.
b. Personal investments by pension or investment fund personnel that parallel investments made on behalf of the organization.
c. Unqualified investment advisors, security representatives, and inept, inexperienced financial services providers.
d. Gifts entertainment and favours from outside advisors and security representatives to pension or investment fund personnel.
e. Privacy and confidentiality breaches connected with pension or investment fund personnel.
f. Churning of investments, high portfolio turnover.
g. Pension or investment fund performance that appears contrary to reliable market indicators.
h. Failure to provide detailed, decision-critical information to pension or investment fund personnel by outside advisors and security representatives.

III.IV Travel Expenses

Organizations spend little time reviewing travel expenses because of the seemingly insignificant value of each item. But small infractions can add up to thousands - and ultimately millions of pesos in large organizations. According to a recent survey, respondents indicated that travel and entertainment fraud was then third greatest controllable cost in their organizations. An organization can become riddled with fraud and abuse if employees believe that the top executives consider it acceptable.

Additionally, quite often travel fraud and abuse can be an indicator of much larger problems such as bribery and kickback schemes and serious conflicts of interest cases. Fraudulent travel reimbursement claims are often used to disguise or hide bribes and kickbacks. A fraudulently prepared travel reimbursement claim can be used to recover the expense incurred in buying a gift, or paying a cash bribe or a kickback.

III.IV.I Common Travel Fraud Indicators

a. Falsified, altered, unusual receipts.
b. Inflated expense amounts.
c. Dummy receipts claiming fictitious expenditures.
d. Unnecessary, unauthorized, unapproved travel.
e. Claiming days of travel that were not travelled.
f. Double-claimed expenditures.
g. Mischaracterized expenses, for example claiming personal expenditures as business expenses.
h. Failing to provide required documentation.
i. Travel expenses claims that are not reviewed.
j. Overstated expenses.

III.V Fraud in Computerized Environment

The number of ways in which fraud in the computer environment is committed, is matched only by the number of ways in which systems are used, the number of systems users, and the numbers of cyber criminals. The following are fraud implications of computer technology and its related vulnerabilities:

a. Data concentration
b. Accessibility of storage medium
c. Obscure audit trail
d. Visibility of records
e. Alteration of programs and data
f. Tampering
g. Network
h. Lack of understanding of computer systems and it technology.
i. Inadequate security features.
j. Lack of internal controls
k. Circumvention of controls

III.V.I Common Computer Area Fraud Indicators

a. Missing computers, and other related assets, programs, and data.

b. Use of computer time by employees and former employees for personal reasons.
c. Changed or altered data by employees.
d. Counterfeited data.
e. Changed programs without committee approval.
f. Altered or deleted master files.
g. Override of internal controls.
h. Evidence of Sabotage.
i. Surveillance of data by unauthorized personnel.
j. Hacking by personnel and outsiders.

RESPONSIBILITIES FOR MANAGING THE RISK OF FRAUD - RISK OWNERSHIP

Principal Accounting Officers

The Principal Accounting Officer (PAO)/Secretary of a Ministry/Division is personally accountable for his/her organisation and its risk management. A framework of senior level delegation is essential to ensure that the responsibility and authority for implementing control actions is clear. A mechanism for reporting to the PAO on risk issues should be established. Managing fraud risks (including internal and external fraud risks) is part of the management of all other risks and the same principles apply.

Senior Management

Overall responsibility for Managing the Risk of Fraud should be allocated to an appropriate senior officer. Their specific responsibilities, which can be formally delegated, will depend to some extent with the level of fraud risk the organisation is exposed to but should include some or all of the following:

- Developing a fraud risk profile and undertaking an annual review of the fraud risks associated with each of the key organisational objectives in order to keep the profile current;
- Establishing an effective anti-fraud policy and fraud response plan, commensurate with the level of fraud risk identified in the fraud risk profile;
- Developing appropriate fraud targets;
- Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;
- Establishing appropriate mechanisms for:
    - Reporting fraud risk issues;
    - Reporting significant incidents of fraud to the PAO;
    - Reporting centrally; and
    - Coordinating assurances about the effectiveness of anti-fraud policies to support the Statement of Internal Control.

- Liaising with the Risk Management Committee and/or Audit Committee as appropriate –where an organisation has a Risk Management Committee it may be appropriate for the reports to go to the PAO via that committee. It may also be helpful to ask the Audit Committee to regularly consider fraud risk management issues and significant instances of fraudulent activity;
- Making sure that all staff are aware of the organisation's anti-fraud policy and know what their responsibilities are in relation to combating fraud;
- Developing skill and experience competency frameworks;
- Ensuring that appropriate anti-fraud training and development opportunities are available to appropriate staff in order to meet the defined competency levels;
- Ensuring that vigorous and prompt investigations are carried out if fraud occurs;
- Taking appropriate legal and/or disciplinary action against perpetrators of fraud;
- Taking appropriate action to recover assets;
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Operational Managers

Outside of any more formal delegation of the above duties, all other levels of management are responsible for:

- Implementing and maintaining effective controls to prevent fraud commensurate with the fraud risk profile, and
- Ensuring compliance with anti-fraud policies and fraud response plan.

Individual members of staff

Individual members of staff have an important role to play in combating fraud. Their responsibilities include:

- Acting with propriety in the use of official resources and in the handling and use of corporate fund whether they are involved with cash or payments systems, receipts or dealing with contractors or suppliers;
- Reporting details immediately to their line manager or other avenue for reporting fraud (e.g. whistle blowing arrangements) if they suspect that fraud has been committed or see any suspicious acts or events.

Internal Audit

The role of internal audit is to deliver an opinion to the Principal Accounting Officer on the whole of an organisation's risk management, control and governance. In relation to fraud this will include the examination of the adequacy of arrangements for managing the risk of fraud and ensuring that the organisation actively promotes an anti-fraud culture.

Internal audit will therefore assist in the deterrence of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in the various segments of an organisation's operations. Internal audit's main responsibility is to ensure that management has reviewed its risk exposures and identified the possibility of fraud as a business risk.

Management has the responsibility for conducting fraud investigations but internal audit may be asked to assist, and in some organisations may have had responsibility for conducting investigations delegated to them. Fraud investigation is an area that requires specialist knowledge and where internal audit has this responsibility they need to develop and maintain appropriate levels of expertise.

PROMOTING AN ANTI-FRAUD CULTURE

Introduction

Fraud prevention involves more than merely compiling anti-fraud policies. It also involves putting in place effective accounting and operational controls and the maintenance of an ethical environment that encourages staff at all levels to actively participate in protecting public money and property. Creating an anti-fraud culture involves:

- Having a clear statement of ethical values;
- Establishing a clear anti-fraud policy and fraud response plan;
- Promoting staff awareness of fraud;
- Recruiting honest staff (checking references etc); and
- Maintaining good staff morale.

Code of Ethics

As stewards of public funds civil servants must have, and be seen to have, high standards of personal integrity. Staff should not accept gifts, hospitality or benefits of any kind from a third party that might be seen to compromise their integrity. All personnel should be reminded that they are bound by a code of ethics which, unless issued separately, should be stated in the anti-fraud policy. The ethics policy will:

- Explain that staff must follow the organisation's rules without circumventing controls;
- Explain what external interests may give rise to conflicts of interest and require any possible conflicts of interest to be declared;
- Define the organisation's policy on receiving gifts from external parties;
- Explain why it is necessary to keep certain information about the organisation confidential;
- Require employees to report suspected fraud to a named individual or via a fraud hotline;
- State that breach of the policy will be treated as a disciplinary offence;

- Provide cross-references to the organisation's anti-fraud policy and fraud response plan.

Fraud Policy

Many organisations use a fraud policy statement to communicate the organisation's approach to fraud. Such a statement may include some or all of the following areas:

- A statement about the organisation's attitude to fraud (e.g. zero tolerance);
- The Code of Ethics;
- Personnel policies (e.g. recruitment policies);
- The allocation of responsibilities for the overall management of fraud;
- Reporting suspicions of fraud, including "hotline" arrangements if used;
- Whistle blowing arrangements;
- The procedures which staff should follow if a fraud is discovered;
- Guidance on training for the prevention and detection of fraud;
- Reference to the response plans that have been devised to deal with and minimise the damage caused by any fraudulent attack.

An example of a fraud policy statement can be found at Appendix 10.

Fraud Response Plan

It is important that managers and others know what to do in the event of a fraud so that they can act without delay. It is recommended that departments prepare a fraud response plan. The objective of a fraud response plan is to ensure that timely and effective action can be taken to:

- Prevent losses of funds or other assets where fraud has occurred and to maximise recovery of losses;
- Minimise the occurrence of fraud by taking rapid action at the first signs of a problem;
- Identify the fraudsters and maximise the success of any disciplinary/legal action taken;
- Minimise any adverse publicity for the organisation, suffered as a result of fraud;
- Identify any lessons which can be acted upon in managing fraud in the future;

- Reduce adverse impacts on the business of the organisation;
- Make people aware of the possible consequences of committing fraud by publicising details of successful actions taken against perpetrators of fraud.

The existence of a fraud response plan may, in itself, help to act as a deterrent as it shows that an organisation is prepared to defend itself against the risk of fraud. **Appendix 11** contains more information about what to include in a fraud response plan.

Promoting Staff Awareness of Fraud

All staffs need to be kept fully informed about the organisation's anti-fraud policy and what part they are expected to play in it. This can be achieved in a number of ways:

- Give every employee a copy of the organisation's ethics/anti-fraud policy as part of their contract of employment or staff handbook;
- Informing new staff during induction training;
- Establishing a training programme and ensuring all staff attend it;
- Making the anti-fraud policy, code of ethics and fraud response plan available to all staff (e.g. via networked IT systems);
- Communicating all changes in policy to all staffs immediately;
- Including fraud matters in a weekly or monthly newsletter;
- Reporting to staff outcomes of investigations and disciplinary action against employees who perpetrate theft or fraud.

Personnel Policies

Personnel recruitment policies play an important role in reducing the risk of fraud. Managers and staff responsible for staff recruitment must adhere strictly to the organisation's recruitment policy, particularly in relation to:

- The screening of references for new employees;
- Special arrangements for sensitive posts (e.g. checking police records);
- Detailed appraisal during probationary periods; and
- Detailed "exit" interviews for employees leaving the organisation.

Maintaining Staff Morale

Managers should try to create the conditions in which staffs have neither the motivation nor the opportunity to commit fraud. The maintenance of good staff morale may help to minimise the likelihood of an employee causing harm to the organisation through fraud.

EXAMPLE OF AN ANTI-FRAUD POLICY

A fraud policy statement should be simple, focused and easily understood. Its contents may vary from organisation to organisation but you should consider including references to the organisation's determination to:

- Take appropriate measures to deter fraud;
- Introduce/maintain necessary procedures to detect fraud;
- Investigate all instances of suspected fraud;
- Report all suspected fraud to the appropriate authorities;
- Assist the police in the investigation and prosecution of suspected fraudsters;
- Recover from fraudsters any assets wrongfully obtained;
- Encourage employees to report any suspicion of fraud.

An example of an anti-fraud policy follows.

Introduction

The [**Organisation name**] requires all staffs at all times to act honestly and with integrity and to safeguard the public resources for which they are responsible. The Department will not accept any level of fraud or corruption; consequently, any case will be thoroughly investigated and dealt with appropriately. The Department is committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level of risk.

What is Fraud?

No precise legal definition of fraud exists. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

"Fraud" is usually used to describe depriving someone of something by deceit, which might either be straight theft, misuse of funds or other resources, or more complicated crimes like false accounting and the supply of false information. In legal terms, all of these activities are the same crime–theft.

Avenues for Reporting Fraud

The Department has in place avenues for reporting suspicions of fraud. Staff should report such suspicions to their line managers, to the department's internal audit (or specialist fraud unit), or to the hotline set up for the purpose. All matters will be dealt with in confidence. Vigorous and prompt investigations will be carried out into all cases of actual or suspected fraud discovered or reported.

Responsibilities

Responsibilities in relation to fraud are set out below:

- The Principal Accounting Officer (PAO)/Secretary of a Ministry/Division is responsible for establishing and maintaining a sound system of internal control that supports the achievement of departmental policies, aims and objectives. The system of internal control is designed to respond to and manage the whole range of risks that a department faces. The system of internal control is based on an on-going process designed to identify the principal risks, to evaluate the nature and extent of those risks and to manage them effectively. Managing fraud risk will be seen in the context of the management of this wider range of risks.
- Overall responsibility for managing the risk of fraud has been delegated to..... [e.g. a senior official]. Their responsibilities include:
    - Developing a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organisational objectives in order to keep the profile current;
    - Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in the fraud risk profile;
    - Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;
    - Establishing appropriate mechanisms for:
        - Reporting fraud risk issues;
        - Reporting significant incidents of fraud to the AO;
        - Reporting centrally; and
        - Coordinating assurances about the effectiveness of anti-fraud policies.
    - Liaising with the Risk Management Committee and/or Audit Committee.

- Making sure that all staff are aware of the organisation's anti-fraud policy and know what their responsibilities are in relation to combating fraud;
- Developing skill and experience competency frameworks;
- Ensuring that appropriate anti-fraud training and development opportunities are available to appropriate staff in order to meet the defined competency levels;
- Ensuring that vigorous and prompt investigations are carried out if fraud occurs or is suspected;
- Taking appropriate legal and/or disciplinary action against perpetrators of fraud;
- Taking appropriate disciplinary action against supervisors where supervisory failures have contributed to the commission of fraud;
- Taking appropriate disciplinary action against staff who fail to report fraud;
- Taking appropriate action to recover assets;
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.
- Operational managers are responsible for:
    - Ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively;
    - Preventing and detecting fraud;
    - Assessing the types of risk involved in the operations for which they are responsible;
    - Reviewing and testing the control systems for which they are responsible regularly;
    - Ensuring that controls are being complied with and their systems continue to operate effectively;
    - Implementing new controls to reduce the risk of similar fraud occurring where frauds have taken place.

Internal audit is responsible for:

- Delivering an opinion to the Principal Accounting Officer on the adequacy of arrangements for managing the risk of fraud and ensuring that the department promotes an anti-fraud culture;
- Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in the various segments of the department's operations;

- Ensuring that management has reviewed its risk exposures and identified the possibility of fraud as a business risk;
- Assisting management in conducting fraud investigations.

Every member of staffs is responsible for:

- Acting with propriety in the use of official resources and the handling and use of public funds whether they are involved with cash or payments systems, receipts or dealing with suppliers;
- Conducting themselves in accordance with the principles of public life;
- Being alert to the possibility that unusual events or transactions could be indicators of fraud;
- Reporting details immediately through the appropriate channel if they suspect that a fraud

  has been committed or see any suspicious acts or events;
- Cooperating fully with whoever is conducting internal checks or reviews or fraud investigations.

Fraud Response Plan

The department has a Fraud Response Plan that sets out how to report suspicions, how investigations will be conducted and concluded. This plan forms part of the department's anti-fraud policy.

Conclusion

The circumstances of individual frauds will vary. The department takes fraud very seriously. All cases of actual or suspected fraud will be vigorously and promptly investigated and appropriate action will be taken.

FRAUD RESPONSE PLANS

A fraud response plan should cover the following areas:

- Instructions on the action required at the point of discovery;
- To whom the fraud or suspicion of fraud should be reported in the first instance, for example this may a line manager, the nominated "appeals" officer within a department, through internal procedures authorised by the employer (e.g. fraud hotline), internal audit department, anti-fraud specialists;
- How the organisation should investigate the fraud and who will lead the investigation.
- Depending on the nature of the fraud special investigators, internal auditors who have been entrained in fraud investigation, techniques or a fraud unit may be used. The facts should be established quickly by the operational managers; any threat of further frauds or losses should be removed immediately, for example, by changing procedures or suspending payments;
- How to secure evidence without alerting suspects at the outset of the investigation;
- How to secure the evidence in a legally admissible form (e.g. evidence must be carefully preserved; it should not be handled and no marks made on original documents; a record should be kept of anyone handling evidence);
- Guidance about dealing with employees under suspicion (e.g. prompt action must be taken; action to suspend or dismiss an employee should be taken in conjunction with the personnel department; employees under suspicion who are allowed to remain on the premises must be kept under constant surveillance; make an immediate search of the suspects work area, filing cabinets, computer files);
- Guidance about interviewing (e.g. decisions about interviewing suspects must be made by senior management; if the Police are to be used they must be involved at an early stage; all interviews must be conducted under properly controlled conditions in order to ensure that any statement taken and subsequently used as evidence in a court case will not be rejected as inadmissible);
- When and how to contact the Police. Any decision about involving the Police must be taken by senior management. A record of police contacts should be recorded in this section;

Members of the public should also be encouraged to report their suspicions of fraud through advertising campaigns, offering rewards, ensuring that avenues for reporting fraud are widely publicised and assuring whistle-blowers that any information received will be treated confidentially.

Computer Assisted Audit Techniques

These can be used to identify unusual types of transaction within a department's records, which might be worth further investigation. Such checks could be built into information systems to provide regular exception reports to managers on transactions.

Investigation and Analysis Tools

These help fraud investigators to handle their case evidence, for example by highlighting links between colluding parties or between fraudulent transactions. These techniques can be used to identify indicators of possible fraud including:

- Duplicate payments;
- Unusual patterns of works orders (e.g. a large number of jobs valued just below the financial limits at which full competition in awarding the work would be employed);
- Invalid VAT numbers or incorrect amounts of VAT;
- Unexpected relationships between sub-contractors (e.g. shared addresses, telephones or fax numbers, bank accounts or directors).

Data mining is a technique that can be used to identify the relationships between sets of data within a department's databases. Some of the patterns identified may indicate fraudulent activity or practices that increase the risk of fraud.

Data matching can be used to compare computer records held for different purposes or by different bodies to identify discrepancies and anomalies. A department, for instance, could compare its data on contractors with similar data held by other public sector bodies to see who have committed fraud to see whether or not they are using the same firms.

Where organisations use data mining or data matching to detect fraud then they need to be aware of the possible restrictions on the way personal data can be used in fraud detection exercises or fraud investigations.

Fraud Indicators

Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity. All they can do is point the way for further detailed investigation. See Appendix 13 for examples of fraud indicators.

EXAMPLES OF FRAUD INDICATORS

A number of frauds can come to light because of suspicions aroused by, for instance, the behaviour of certain individuals. Managers and staff should also be alert to any warning signs that might indicate that fraud is taking place. These may be:

- Staff under stress without a high workload.
- First to arrive in the morning, last to leave at night.
- Egotistical (e.g. scornful of system controls).
- A risk taker or rule breaker.
- Reluctance to take leave.
- Refusal of promotion.
- Unexplained wealth.
- Sudden change of lifestyle.
- New staff resigning quickly.
- Cosy relationships with suppliers/contractors.
- Suppliers/contractors who insist on dealing with one particular member of staff.
- Disgruntled at work, a complainer.
- Greedy or has genuine financial need.

To spot fraud indicators in individual areas or activities it is important that accepted practices have been established for the area or activity under review and that the auditor is familiar with them. The following are examples of possible fraud indicators in a number of areas.

- Unusual employee behaviour (e.g. a supervisor who opens all incoming mail, refusal to comply with normal rules and practices, fails to take leave, managers by-passing subordinates, subordinates by-passing managers, living beyond means, regular long-hours working, job dissatisfaction/unhappy employee, secretiveness or defensiveness).
- Key documents missing (e.g. invoices, contracts).
- Inadequate or no segregation of duties.
- Absence of controls and audit trails.
- Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation).

- Documentation that is photocopied or lacking essential information.
- Missing expenditure vouchers and official records.
- Excessive variations to budgets or contracts.
- Bank and ledger reconciliations are not maintained or cannot be balanced.
- Excessive movements of cash or transactions between accounts.
- Numerous adjustments or exceptions.
- Overdue pay or expense advances.
- General ledger out of balance.
- Duplicate payments.
- Ghost employees on the payroll.
- Large payments to individuals.
- Crisis management coupled with a pressured business environment.
- Lack of established code of ethical conduct.
- Lack of Senior Management oversight.
- Unauthorised changes to systems or work practices.
- Lack of rotation of duties.
- Policies not being followed.
- Post Office boxes as shipping addresses.
- Lowest tenders or quotes passed over with minimal explanation recorded.
- Single vendors.
- Unclosed but obsolete contracts.
- Defining needs in ways that can be met only by specific contractors.
- Splitting up requirements to get under small purchase requirements or to avoid prescribed levels of review or approval.
- Vague specifications.
- Disqualification of any qualified bidder.
- Climate of fear or an unhealthy corporate culture.
- High staff turnover rates in key controlling functions.
- Chronic understaffing in key control areas.
- Low staff morale/lack of career progression/weak management.
- Excessive hours worked by key staff.
- Consistent failures to correct major weaknesses in internal control.
- Management frequently override internal control.

- When an employee is on leave, the work is left until the employee returns.
- Lack of common sense controls such as changing passwords frequently, requiring two signatures on cheques or restricting access to sensitive areas.
- An employee's lifestyle is more affluent than would be expected from his/her employment.

REDUCING OPPORTUNITIES FOR FRAUD

Introduction

Managers must ensure that the opportunities for fraud are minimised. Separation of duties, effective procedures and checks should prevent or deter fraud from occurring. Opportunities to commit fraud may be reduced:

- By ensuring that a sound system of internal control proportional to risk has been established and that it is functioning as intended;
- Through the "fear factor" (i.e. the risk of being caught or the severity of the consequences);
- By changing attitudes to fraud;
- By making it too much effort to commit.

Internal Control

"Control" is any action, procedure or operation undertaken by management to increase the likelihood that activities and procedures achieve their objectives. Control is a response to risk – it is intended to contain uncertainty of outcome.

Some frauds arise because of a system weakness such as a lack of proper control over e.g. placing of purchase orders. Other frauds are the result of failures to follow proper control procedures. It may be the result of carelessness in carrying out a check, or it may be that too much trust has been placed in one individual with no effective separation of duties. Frauds that result from collusion may be more difficult to detect and prevent as these types of fraud tend to operate within the normal control environment.

In designing control, it is important that the control put in place is proportional to the risk. In most cases it is normally sufficient to design control to give a reasonable assurance of confining loss within the risk appetite of the organisation. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking the purpose of control is to contain risk to a reasonable level rather than to remove it entirely.

When risks and deficiencies in the level of control are identified it is necessary to choose the most appropriate type of controls within the above guidelines. In respect of fraud risks,

prevention is almost always preferable to detection. Strong preventive controls should therefore be applied wherever possible.

The following range of controls should be considered always ensuring that a balance between identified risk and value for money is maintained:

Physical security: this is a preventive measure which controls or monitors access to assets, documentation or IT systems to ensure that there is no unauthorised use, loss or damage. Assets can range from the computer terminal that sits on the desk to the cheques sent out to pay suppliers. As a general principle all assets should be held securely and access to them restricted as appropriate. The control should apply not only to the premises but also to computers, data bases, banking facilities, documents and any other area that is critical to the operation of the individual organisation. It may even be appropriate to restrict knowledge of the existence of some assets.

Access to computer systems is an important area that should be very tightly controlled, not only to prevent unauthorised access and use, but also to protect the integrity of the system. The threat to computers can come from both inside and outside an organisation. This threat may increase with the introduction of systems which allow the public to do business electronically with government departments. Computers are also vulnerable to theft, both in terms of hardware and software. This type of theft has the additional cost of potential major disruption to the core operations of an organisation.

Organising: organising involves the allocation of responsibility to individuals or groups so that they work together to achieve objectives in the most efficient manner. Major principles in organising relevant to fraud are:

- Clear definition of the responsibilities of individuals for resources, activities, objectives and targets. This includes defining levels of authority. This is a preventive measure which sets a limit on the amounts which may be authorised by individual officers. To be effective, checks need to be made to ensure that transactions have been properly authorised;
- Establishing clear reporting lines and the most effective spans of command to allow adequate supervision;
- Separating duties to avoid conflicts of interest or opportunities for abuse. This is also largely a preventive measure which ensures that the key functions and controls over a process are not all carried out by the same member of staff (e.g. ordering goods

should be kept separate from receipt of goods); similarly authorisation and payment of invoices; and

- Avoiding undue reliance on any one individual.

Supervision and checking of outputs: supervision is the function by which managers scrutinise the work and performance of their staff. It provides a check that staff are performing to meet standards and in accordance with instructions. It includes checks over the operation of controls by staff at lower levels. These act as both preventive and detective measures and involve monitoring the working methods and outputs of staff. These controls are vital where staff are dealing with cash or accounting records. Random spot checks by managers can be an effective anti-fraud measure.

Audit trail: this is largely a detective control, although its presence may have a deterrent effect and thus prevent a fraud. An audit trail enables all transactions to be traced through a system from start to finish. In addition to allowing detection of fraud it enables the controls to be reviewed.

Monitoring: management information should include measures and indicators of performance in respect of efficiency, effectiveness, economy and quality of service. Effective monitoring, including random checks, should deter and detect some types of fraudulent activity.

Evaluation: policies and activities should be evaluated periodically for economy, efficiency and effectiveness. The management of the operation may perform evaluations, but they are usually more effective when performed by an independent team. Such evaluations may reveal fraud.

Staffing: adequate staffing is essential for a system to function effectively. Weaknesses in staffing can negate the effect of other controls. Posts involving control of particularly high value assets or resources may need the application of additional vetting procedures. Rotation of staff between posts can help prevent or detect collusion or fraud.

Asset accounting: asset registers used for management accounting purposes can help detect losses that may be caused by fraud.

Budgetary and other financial controls: use of budgets and delegated limits for some categories of expenditure and other accounting controls should ensure that expenditure is properly approved and accounted for by the responsible manager. This should limit the scope for fraud and may result in some types of fraud being detected.

Systems development: controls over the development of new systems and modifications to existing systems or procedures are essential to ensure that the effect of change is properly assessed at an early stage and before implementation. Fraud risks should be identified as part of this process and the necessary improvements in control introduced.

These are only some examples of the types of control that can be used to prevent or detect fraud. For examples of internal controls in specific areas see Appendix 15.

The "Fear Factor"

Major deterrents to perpetrating fraud are the risk of being caught and the severity of the consequences. The most important fact about deterrence is that it derives from perceived risk and not actual risk. A department may manage to increase the actual risk of detection but it will only achieve a deterrent effect if it ensures that perceptions of risk change too. Ways in which departments can do this include:

- Warnings on forms such as: "false statements may lead to prosecution";
- General publicity;
- Increasing the severity of penalties;
- Always taking appropriate action against known perpetrators of fraud.

Changing Attitudes to Fraud

The most effective strategies designed to change attitudes rely on motivation rather than fear. They aim to persuade people of the undesirability of a particular behaviour. Attitude changing strategies rely to a large extent on publicity campaigns to achieve their effect so it is important that departments carry out a full appraisal of the benefits of any proposed advertising campaign and to establish some way of measuring the outcomes of such campaigns. Departments need to be clear about the objectives and targets of their campaigns.

RISKS AND CONTROLS IN SPECIFIC SYSTEMS

Risks associated with cash handling

There are many risks associated with cash handling. Theft or misappropriation of cash may be assisted by the suppression, falsification or destruction of accounting records, or where no initial records are created at all. This section suggests some controls that should be in place.

How fraud could be committed	Examples of controls
Theft	• Cash should be held securely at all times. • Access to cash should be restricted to named personnel. • Controls over keys should be set up and keys should only be issued to authorised personnel. • Cash balances in hand/chest should be kept to a minimum authorised specified balance, recorded and checked periodically. • Excess cash be deposited to authorised bank account timely.
Income received not brought to account	• Always issue pre-numbered receipts. • Maintain accurate records of income received. • Post opening duties should be carried out by at least two people and a receipts log completed and signed by both officers. • Separate duties at key stages of the process: - post opening and logging of receipts; - bringing receipts to account and preparation of cash and cheques for banking; - daily cash balancing and bank reconciliations. • Regular and random management checks of source documentation, accounting records and bank reconciliations; • Rotation of staff.
Illegal transfer or diversion of money. **Changes and additions to payee**	• Changes and additions to payee standing data should be independently authorised.

How fraud could be committed	Examples of controls
standing data details.	• System access to make and authorise these changes should be carefully restricted and logged. • Provide adequate supervision of all staff particularly new, inexperienced or temporary staff. • All payments should be independently authorised before they are made. • Restrict knowledge of transfer codes (and passwords if payments are initiated internally by computer) to approved personnel. Transfer codes and passwords should be changed frequently and always when staff leave. • Payment reports should be independently reviewed for accuracy immediately before the transfer of funds occurs. • Separation of duties between those setting up payment accounts and those authorised to trigger payments should be maintained at all times. Similarly separate duties of receiving goods and services from the process of making payment.
False creation of or unauthorised updates to accounting records to allow the unauthorised payment of funds	• Amendments and deletions to accounting records should be independently authorised. These should be evidenced by signature, together with name and grade. • Independent checks to ensure amendments have been carried out correctly. These should be evidenced by signature, together with name and grade. • Authorisation levels and frequency of checks, including the use of spot checks, should depend on: - the amounts involved; - the degree of risk associated with the system. • Accounting records and petty cash should be reconciled on a regular basis. These reconciliations should be recorded and independently reviewed. Discrepancies should be investigated and resolved. • Any discrepancies that cannot be resolved or any losses that have occurred should be reported as part of a formally

How fraud could be committed	Examples of controls
	defined process. • Suspense accounts should be reviewed on a regular basis to confirm their validity.
Falsification and duplication of invoices in order to generate a false payment	• There should be segregation of duties between ordering and payment of invoices. • Checks for duplicate invoices should be carried out periodically. • Invoices should be checked back to orders for evidence that the orders were genuine and properly authorised.
Unauthorised use of cheques and payable orders	• Financial stationery should be held securely and records kept of stock holdings, withdrawals and destruction of wasted stationery. • Signatories and delegated powers should be established for cheques and payable orders. • Cheques and payable orders should be checked to source documentation before issue. • Use restrictive crossings such as "non-transferrable" and "A/c Payee". • Ensure that addresses to which payable instruments are sent are correct. For large value payments check encashment to ensure that the intended recipient did receive the payment. • Discourage the fraudulent amendment of cheque details by careful choice of inks and printers so that the print produced on cheques is as indelible as possible. • Print the amount in figures as close to the £ sign as possible. • Write payee details in full rather than use abbreviations or acronyms. • Fill up blank spaces with insignificant characters such as asterisks. • Use envelopes that make it less obvious that they contain cheques for mailing purposes. • Ensure that signed cheques are not returned to payment staff. • Reconcile bank statements with cheque listings regularly.

Risks associated with payroll

Risks that may be associated with the payroll function include the introduction of non-existent (ghost) employees, unauthorised amendments made to input data, and the payment of excessive overtime, bonus or travel claims. This section suggests some controls that should be in place.

How fraud could be committed	Examples of controls
Creating fictitious employees whose pay is then obtained by the frauds error by someone in collusion or obtaining pay that is not consistent with employee grade	• Ensure that, wherever possible, all other payroll changes are made by a personnel function that is organisationally separate from payroll function. Only Personnel should be able to authorise changes to the payroll. • Ensure that all new appointments not subject to recruitment by a separate Personnel function (including part-time and casual staff) and changes to standing data (e.g. new pay rates) are approved and separately authorised by the employing department and by Personnel who should independently confirm the existence of starters and that rates of pay to be paid to starters are correct. • Produce listings of all starters, leavers and changes to standing data as part of every payroll run. At least a sample should be checked by Payroll section and a further random sample checked by management. • Produce regular exception reports (e.g. emergency tax codes for more than 6 months, no personal numbers, and duplicate payees) for investigation by management. • Subject the payroll master file to periodic checks by personnel to ensure that each post is

How fraud could be committed	Examples of controls
	authorised, that the correct person is in post, that the person exists and that the basis of salaries and allowances are correct.
Making false claims for allowances, travel and subsistence	• Establish a comprehensive set of travel and subsistence rules and ensure that they are communicated to staff. • Establish a formal process that involves line managers approving and reviewing work plans and programmes for visits, especially for staff where there is no countersigning requirement. • Institute checks by countersigning officers of claims against approved work plans, standard mileages for regular destinations and primary evidence such as hotel bills, rail tickets and taxi receipts. • Ensure that countersigning officers pass approved claim forms direct to the finance team. • Instruct countersigning officers to initial and amendments to details on claim forms and finance teams to reject any claims where amendments have not been initialled. • Instruct finance teams to ensure that correct rates are claimed, substantiating documents (e.g. hotel invoices) are included and to compare counter signatures on claims against sample signatures provided by authorised counter- signatories. • Random management checks should be carried out to verify details on claims and to ensure that finance team checks are applied rigorously to claims. • Budget holders should be provided with sufficient information to enable them to monitor travel costs against budget.

Risks associated with grant funding

This section sets out examples of the controls that should be in place to counter the fraud risks specifically associated with payment of grants

How fraud could be committed	Examples of controls
Grant funds are misappropriated	• Strict guidelines on the claims procedures should be established and communicated to all staff employed to process claims, especially new recruits. • Delegated authorities and levels of authorisation should be established. • Claims should be assessed to determine their complexity and level of risk and allocated accordingly to officers with the relevant experience and expertise. • All claims and supporting evidence should be checked for accuracy, completeness and timeliness. • No single officer should be involved in processing and authorising a complete claim and appropriate segregation should be maintained throughout the process. • Good quality case records should be maintained. • An officer with the appropriate delegated authority should give the final approval for a claim. • Training needs should be assessed periodically and appropriate training plans drawn up. • All claims relating to an individual or organisation should be identified and cross-referenced to reduce the risk of duplicating payments. • Periodic reassessments should be carried out where on-going claims are concerned. • Copies of all outgoing correspondence should be traceable to the originating officer. • Liaise with other grant making organisations to check application data and to avoid making payments where the payment of other grants mean that claimants are not entitled to them. • Reports of grant payments should be regularly scrutinised to ensure that only approved grants have

	statement that you are certain you did not make, contact your card issuer immediately. • Check that you are fully aware of any payment commitments you are entering into, including whether you are instructing a single payment or a series of payments. • Never disclose your card's PIN to anyone, including people claiming to be from your bank or the Police, and NEVER write it down or send it over the Internet. • If you have any doubts about giving your credit card details find another method of payment.

Risks associated with the use of contractors

The section sets out some examples of controls which should be in place, in addition to those which apply generally to cash handling and purchasing systems, to counter the fraud risks faced in relation to the use of contractors:

How fraud could be committed	Examples of controls
A contractor could be selected as a result of favouritism or who does not offer the best value for money	• Draw up and agree clear and comprehensive specification. • Seek tenders from suitable suppliers. • Draw up clear and comprehensive tender evaluation criteria. • Tenders should be delivered to those responsible for selection without interference. • Late tenders should not be accepted. • Tenders should be evaluated by a tender evaluation board against the agreed evaluation criteria. • Ensure compliance of the directives of PPR where applicable. • The tender that offers the best value for money should be recommended for acceptance. • The Project Board should approve the successful contractor.

How fraud could be committed	Examples of controls
	• Staff should be required to declare any personal interests they may have which may affect the tendering process.
Payments made for work not carried out as a result of collusion between the contractor and the official	• Invoices are paid only when accompanied by independent certification that work has been satisfactorily carried out. • There is a register of contracts in progress. • Contracts are only added to the contract register when properly approved and authorised. • Invoices are only accepted from approved contractors. • All contract variations are authorised, documented, variation orders are sequentially numbered, produced in an agreed format and authorised before payment. • Checks are made against budget and planned expenditure prior to approval of payment.

Risks associated with assets

Risks in this area include use of assets for personal gain, or misappropriation of assets. This section suggests some controls that should be in place to counter those risks.

How fraud could be committed	Examples of controls
Theft or unauthorised use of assets	• Asset registers to be maintained up to date. • Inventories to be used, where possible, and assets assigned to individual budget centres. • There is adequate definition of assets on the asset register. • Asset marking to be carried out where possible. • Physical security of assets to be maintained. • Spot checks on existence of assets to be carried out on a regular basis.

Annexure

Annex – A

FRAUD RISK REGISTER GUIDANCE

What is a fraud risk register?

It is a register or listing of fraud risks and fraud risk assessments and responses.

It is a key procedural tool in preventing fraud and very importantly facilities a 'resources to risk' approach which provides for the allocation of scarce resources to address the areas of highest fraud risk.

What is 'fraud risk'?

Fraud risks the risk of fraud taking place.

What is fraud risk assessment?

It is the relative and combined assessment of the LIKELIHOOD and IMPACT of fraud taking place. It facilitates a systematic and proportionate response to the risk of fraud taking place.

The likelihood of fraud and the impact of fraud taking place may be assessed as LOW, MEDIUM or HIGH.

It is a largely qualitative assessment.

Grading of combined assessment of Likelihood and Impact of fraud taking place

		Impact		
		low	medium	high
Likelihood	low	E	D	C
	medium	D	C	B
	high	C	B	A

A high likelihood and high impact of fraud taking place produce a grading of A whereas low likelihood and low impact produce a grading of E.

For each grade of risk there is an appropriate proportionate response.

Response to fraud risk assessment	
Grade	**Risk mitigation actions**
A	Mitigation actions to reduce the likelihood and seriousness to be identified and implemented as soon as possible.
B	Mitigation actions to reduce the likelihood and seriousness to be identified and appropriate actions implemented as priority two.
C	Mitigation actions to reduce the likelihood and seriousness to be identified and costed for possible action if funds permit.
D	To be noted - no action is needed unless grading increases over time.
E	To be noted - no action is needed unless grading increases over time.

Format of risk register

Risk Register for: X

Last updated: Y

ID	Description of Risk [1]	Likelihood [2]	Impact [3]	Grade [4]	Change [5]	Mitigation Actions [6]	Responsible Officer [7]	Cost [8]
1.1								
1.2								

(1) Description of risk

The description of the risk should be a summary description of the risk of fraud taking place.

(2) Likelihood

The likelihood of fraud taking place may be assessed as LOW, MEDIUM or HIGH. It is a relative rather than absolute assessment.

The assessment of likelihood requires an assessment of the strength of controls in place to prevent fraud taking place such as the division of duties and supervisory checks.

(3) Impact

The impact of fraud taking place may be assessed as LOW, MEDIUM or HIGH.

The assessment of the impact of the fraud taking place should not simply take account of the financial impact but should also consider the organisation's reputation.

(4) Grade

Please see the grading table above.

A high likelihood and high impact of fraud taking place produce a grading of A whereas low likelihood and low impact produce a grading of E.

The recommended mitigating action for a grade A risk is 'Mitigation actions to reduce the likelihood and seriousness to be identified and implemented as soon as possible' whereas the recommended action for a grade E risk is 'To be noted - no action is needed unless grading increases over time'.

This approach facilitates a systematic and proportionate response to the risk of fraud taking place.

(5) Change

This records the change in the grading of the risk. Regular updating of the risk register facilitates the monitoring of the changing nature of the risk of fraud.

(6) Mitigating actions

This records the mitigating actions required.

(7) Responsible officer

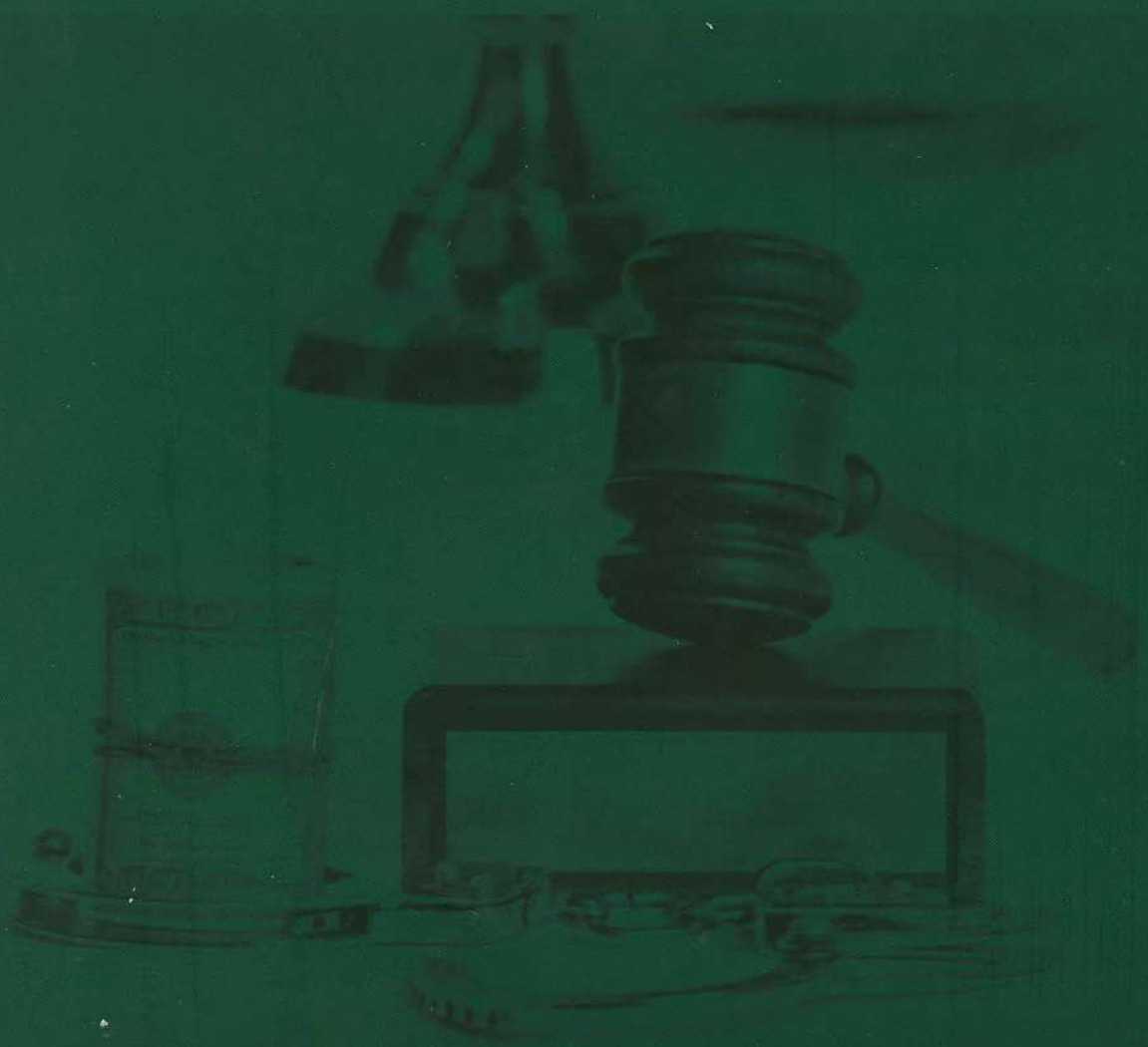
This records the officer responsible for managing the risk and implementing the mitigating actions required. It facilitates the allocation of the ownership of fraud risks. It also provides a basis for holding the responsible officer accountable.

(8) Cost

This column records any costs associated with the required mitigating action.

Summary

The risk of fraud and the required mitigating action and responsible persons are documented in a formal, comprehensive, systematic, structured and prioritised way.



SPEMP
Strengthening Public Expenditure Management Program
MAKING PUBLIC MONEY COUNT

SPEMP-B : Strengthening the Office of the Comptroller and Auditor General
Address : Audit Complex (11th Floor), Segunbagicha, Dhaka-1000
Phone : +88 02 8391274-77, PABX : +88 02 8391277
Fax : +88 02 8391276

design & print
RMC/01712 766221