For Official Use

Management of Risk of Fraud in Government

A Good Practices Guide

CENTRE FOR GOOD GOVERNANCE™
Knowledge • Technology • People

Disclaimer

Good practices are meant to be shared and emulated. The compilation of Good Practices contained in this volume is based on material available in public domain. A list of books, articles, etc. consulted in preparing the Good Practices is given at the end of the volume. Originality, if any, in preparing the Good Practices lies only in their arrangement and adoption to suit our requirements. This compilation is intended strictly for use by government offices and other parastatal organizations.

For Official Use

Management of Risk of Fraud in Government

A Good Practices Guide

CENTRE FOR GOOD GOVERNANCE™
Knowledge • Technology • People

Acknowledgments

The Good Practices Guide has been prepared by Mr A Srinivas Kumar, IA&AS, Dy. Executive Director and Ms. P Vasantha, Knowledge Manager under the leadership of Dr. Rajiv Sharma, IAS, Director General, Centre for Good Governance.

This project has been undertaken with funds provided by Foreign and Commonwealth Office, U.K. under Strategic Programme Fund. We are grateful to the British High Commission for providing the funds and to Ms. Deepa Sundaram, Programme Manager (till July 2008) and Ms. Sudipta Bhadra, Programme Manager - Economic Governance, British High Commission, New Delhi for their constant support and guidance.

We are thankful to Government of Andhra Pradesh, particularly to Mr. J P Murty, IAS, Special Chief Secretary, General Administration Department, for supporting the project by agreeing to implement any practicable measures that the study might suggest.

We wish to record our deep sense of gratitude to Mr C R Kamalnathan, IAS (Retd), Former Vigilance Commissioner, Andhra Pradesh for sharing his vast knowledge and insights on the subject and for adding tremendous value through his comments on the draft of this Guide.

We wish to express our deep sense of gratitude to the following for generously sharing their time in explaining the existing practices in management of fraud: Ms. K.Damayanthi, IAS, Secretary to the Vigilance Commissioner, Mr. S.K.Jayachendran, IPS, DG & Ex-officio Principal Secretary, Vigilance & Enforcement, Mr. N. Madan Mohan, IPS, IGP(Admn.), Vigilance & Enforcement, Mr. N. Balasubramanyam, IPS, DIG, Vigilance & Enforcement, Mr. T. Vivek, Addl.Director, Revenue, Vigilance & Enforcement, Mr. P.Simhadri, Addl. Director, Social Welfare, Mr. Ramesh Chandra, MD, APSCCFC, Mr. Bikshapati, Project Manager-E-procurement, IT&C, Mr. C.L.N.Gandhi, Jt Commissioner, Road Transport Authority, Mr. Haranath Reddy, Vigilance Officer, APVVP.

CGG conducted a workshop on 26 February 2009 to discuss the legal and institutional framework and the suggested good practices. We thank the following participants of the workshop for their valuable inputs: Mr. G N Sunder Raja, IA&AS, Principal Accountant General, Andhra Pradesh, Mr. L V Subramaniam, IAS, Principal Secretary (Health) GoAP, Mr. S K Joshi, IAS, Principal Secretary, Irrigation, GoAP, Mr. K Deenabhandhu, IAS, Principal Secretary, Revenue, GoTN, Mr. Rajiv Trivedi, IPS, Director General, AP Police Academy, Ms. A R Anuradha, IPS, Inspector General of Police, Directorate of Vigilance and Enforcement, Mr. P Dash, Additional Secretary, Industries, Govt. of Orissa, Mr. A R Srinivas, Dy SP, Anti-Corruption Bureau, GoAP, Mr. Arun Manuja, Senior Financial Management Specialist, World Bank, Delhi, Mr. Peter Evans, Senior Governance Adviser, DFID India, Delhi and Mr. Sharad, Chartered Accountant.

While many persons have contributed to making this Good Practices Guide for Managing Risk of Fraud in Government possible, we take full responsibility for any deficiencies in it. We would welcome any suggestions for improving the Guide. You can send your comments to CGG or email them to askumar@cgg.gov.in.

Contents

1. Introduction

Fraud is an unlawful advantage gained by a person through deceit or concealment. Fraud results in significant losses to the public exchequer and adversely affects service delivery. Fraud, like corruption, deprives the community of resources which would otherwise have been available for improving systems and providing better services. Fraud in certain sensitive areas (e.g. issue of passports) may adversely impact the security of the country. It is seen that corruption draws a lot of attention in media and otherwise. Transparency International's corruption perception index is closely followed from year to year. There is a specific law viz. Prevention of Corruption Act and institutions such as Central Vigilance Commission that address the risk of corruption. Whereas, fraud is not subjected to the same notice although a casual glance at reports of Comptroller and Auditor General, Vigilance Commissions and media shows that governments are all the time losing substantial amounts due to fraudulent activities. Given below are a few randomly selected excerpts from different reports.

- *Refund cheques sent by district offices of a national programme to the project director's office are fraudulently deposited in personal bank accounts of an employee. Estimated value: Rs 40 crore.*
- *Social welfare scholarship meant for post-matriculate students of weaker sections misappropriated through forged bills. Estimated Value: Rs 50 crore.*
- *Nine schools run by NGOs in one district misappropriate government funds under the National Child Labour Project by manipulating attendance of children.*
- *Audit scrutiny of records of mid day meal scheme shows that there is a shortage of 0.32 lakh quintals of rice valuing Rs.4.34 crore in distribution.*
- *A pharmaceuticals firm, whose samples are rejected by the State Level Purchase Committee as they fail to meet the required specifications, supplies medicines through an intermediary and at higher prices.*
- *Pay and allowances amounting to Rs.19.07 crore are drawn in excess over a period of 75 months through the pay bills by inflating the number of employees, especially constables.*
- *Rice amounting to 5,271.99 quintals valued at Rs.52.11 lakh for distribution as relief to the people of the district affected in the floods is short received or not received.*

- *Executive Engineer obtains civil works from government departments and misappropriates funds by depositing them in bank accounts opened in his name or with his designation.*

Besides numerous such small value opportunistic frauds committed by individuals, there are also serious frauds involving organized effort, complex operations and huge amounts such as the Stamp Paper Scam. Although losses due to fraud are common and they add up to sizable sum, there have been no systematic efforts to collect data, practices, etc. It is seen that most government departments do not have any formal approach to managing fraud. Sometimes even basic checks and balances (internal controls) are lacking and obvious fraud indicators (red flags) are ignored. Lessons learned from one experience are not internalized through improvement in systems.

In some developed countries, on the other hand, there is a continuous effort to estimate and assess likely frauds and address the risk by taking suitable measures. The UK Department for Work and Pensions, for instance, estimated (2002-03) that losses on account of fraud were £ 490 million on income support and £130 million on Jobseekers' allowance (6.4 percent of expenditure on these benefits of around £9.7 billion)[1]. Prescription fraud alone was estimated to deprive National Health Service, UK of £ 150 million. There are several practice guides such as *The Orange Book – Management of Risk – Principles and Concepts (October 2004) and Managing the Risk of Fraud – A Guide for Managers (May 2003)* brought out by Her Majesty's Treasury, U.K. for government managers to deal with fraud. Several key departments have counter fraud units.

This Good Practices Guide attempts to

a. create awareness about risk of fraud; and

b. *provide certain good practices to manage the risk of fraud.*

By doing so, it seeks to also address the wider issue of improving financial management. The Guide provides a set of formal 'Should-Do' action points for controlling fraud in government organizations. It should be possible for government departments and organizations under them to follow most of the practices immediately and others in due course.

Who can use this Guide?

This Guide is intended for use both by government departments and agencies (societies, corporations, companies, etc.) that work under them.

Due to diverse nature of organizations, one standardized approach to dealing with fraud would be not practicable. However, there are many practices such

[1] *Good Practice in Tackling External Fraud, National Audit Office, U.K.*

as adopting a strategic and risk based approach to dealing with fraud, which would be common to most organizations. This Guide provides a set of practices that are common to all departments and government agencies. Departments / agencies should supplement these practices with those required by the specific nature of their operations.

While all levels of government have to deal with fraud, the relative concerns would naturally differ. The government at the top level (Chief Secretary / Secretary) would be concerned more with taking strategic approach to dealing with fraud. It would, for instance, adopt and promulgate a fraud policy for the government as a whole; enable an environment where swift investigation and conviction, and recovery of money are possible; for this, it will implement required legal and administrative measures such as bringing about changes in laws, rules, etc. and building capacity of government officers involved in investigating to competently handle fraud cases so that they are speedily resolved.

On the other hand, heads of department and agencies below them have a responsibility to assess fraud risks facing the department / organization and ensure that specific anti-fraud measures are in place to show those seeking to defraud the government that such action is unacceptable and will not be tolerated. They would need to constantly monitor the effectiveness of anti-fraud measures.

The actual controls or anti-fraud measures would operate in the field offices where transactions take place. The heads of these field units should guarantee that the anti-fraud measures are effective in actual practice.

As can be seen from above, the top management shares a larger responsibility in tackling fraud in government / organization. Anti fraud culture is driven from the top. The tone set by the top management is critical for mitigating risk of fraud in government.

Level in the Government	***Responsibilities***
Chief Secretary / Secretary	*a. Adopt and promulgate anti-fraud policy for the government as a whole;* *b. Create an enabling environment for swift investigation, conviction, and recovery of money;* *c. Monitor effectiveness of fraud measures by examining cases of fraud reported by internal and external audit and vigilance commission.* *d. Build capacity of government officers involved in investigating to competently handle fraud cases so that they are speedily resolved.*
Head of the Department or	*a. Create anti-fraud culture* *b. Assess fraud risks facing the department / organization;*

an agency below	*c. Ensure that specific anti-fraud measures are in place to deal with the fraud risk;* *d. Identify red flags / alerts and take suitable remedial steps;* *e. Constantly monitor the effectiveness of anti-fraud measures*
Head of Field Office	*a. Guarantee that the anti-fraud measures are effective in actual practice*

Before the actual practices are listed, an attempt has been made to, firstly, clarify the scope of the term ‘fraud’ for the purpose of the good practices guide in Section 2 as the word fraud is used to mean collusive corruption, white collar crimes and economic offences. In Section 3 and 4, a brief overview is given of legal and institutional frameworks respectively. In so far as legal framework is concerned, the important laws in respect of fraud and economic offices are all central legislations. There would be a few state legislations such as Revenue Recovery Act. The subordinate legislation comprising the Rules and Codes are also state specific. The legal framework at the state level in Section 3 refers to the one available in Andhra Pradesh. However, the state level legal framework in other states would be more or less the same. Similarly, the institutional framework at the state level refers to one prevailing in the state of Andhra Pradesh. The institutional framework in other states would also be more or less the same.

2. Defining Fraud

Corruption

Corruption 'involves behaviour on part of the officials in the public sector, whether politicians or civil servants, in which they improperly and unlawfully enrich themselves, or those close to them, by misuse of the public power entrusted to them.' *(Transparency International, 1996)*

The term 'corruption' is used as a shorthand reference for a large range of illicit or illegal activities (Asian Development Bank). The Bank defines corruption as 'the abuse of public or private office for personal gain.' A more comprehensive definition is: 'corruption involves behavior on the part of officials in the public and private sectors, in which they improperly and unlawfully enrich themselves and/or those close to them, or induce others to do so, by misusing the position in which they are placed.'

Many definitions of corruption include fraud thus collapsing the distinction between fraud and corruption. '….fraud and corruption are linked. However they are not the same, rather they are like two concentric circles that overlap in some areas but are separate in others. You can have fraud and no corruption. You can have corruption and no fraud. But where there is fraud there is often corruption' (OECD/ADB 4th Anti-corruption conference).

Fraud

Fraud is defined as 'a legal concept, which involves acts of deceit, trickery, concealment, or breach of confidence that are used to gain some unfair or dishonest advantage; an unlawful interaction between two entities, where one party intentionally deceives the other through the means of false representation in order to gain illicit, unjust advantage.' (*XVI International Conference of Supreme Audit Institutions (INCOSAI) Uruguay, 1998*).

Internal, external and collusive fraud

While an *internal fraud* is one where an employee of the organization commits fraud an '*external fraud* is where third parties, such as businesses, individuals or organized crime groups, steal money from a department or agency, either by obtaining payments to which they are not entitled or keeping monies that they should pay over to the department. Frauds are opportunistic attempts by individuals or businesses to obtain financial advantage.' (*A Guide to good practice in tackling external fraud, National Audit Office, U.K.*) *Collusive* *fraud* is where fraud by a third party is facilitated by an insider i.e. the employee who receives a kickback for the assistance he renders.

White Collar Crime and Economic Offence

White collar crime is described 'as a crime committed *in the course of one's occupation* by a member of the upper class of society.[2]' Example: A manufacturer of drugs deliberately supplying sub standard drugs or a big corporation fraudulently evading tax. A cashier forging cheques or misappropriating cash is a white collar crime. Whereas, a person smuggling a dutiable item is not a white collar criminal in the above sense as there is no connection between his occupation and the crime. It will be simply an economic offence.

Salient features of white collar crimes and economic offences are:

a. Motive of the criminal is avarice (not lust or passion)

b. Background of the crime is non-emotional

c. The victim is usually the state or a section of the public

d. Mode of operation is *fraud* not force

e. Usually the act is deliberate and willful

f. It adversely affects the community's interest in preserving wealth or health of its individual members and national resources, and general economic system from exploitation and waste

The most important feature of these offences is the fact that they do not involve an individual direct victim but are punished because they harm the whole society[3]. In economic terms, white collar crime typically has diffuse costs (to society) and concentrated benefits (for the perpetrators)[4].

Generally speaking, fraud, social offences, economic crimes, white collar crimes, financial fraud and corruption are sometimes used interchangeably, although as seen above there are some important differences between them.

In the table 2 below, an attempt is made to look at different criminal activities and map them against different categories or types of offences. As can be seen, an economic offence may involve fraud as also corruption. White collar

[2] *(Law Commission of India – Forty-Seventh Report on Trial and Punishment of Socio-Economic Offences (1972)*

[3] *(Law Commission of India – Forty-Seventh Report on Trial and Punishment of Socio-Economic Offences (1972)*

[4] Allan Castle, Director The international Centre for Criminal Law Reform and Criminal Justice Policy, Canada

crimes would invariably involve fraud or corruption. In a sense, white collar crimes are a subset of fraud and corruption. It would be evident from the above that a case of fraud may involve an economic offence or be a white collar crime or it could be associated with collusive corruption. A fraud may not involve public exchequer but be between private individuals such as the chit fund fraud, credit card fraud, etc. Misappropriation, embezzlement and forgery could take place in government and also in private sector.

The present Good Practices Guide deals with only fraudulent activities, committed by employees themselves or outsiders, which result in loss to exchequer. It recognizes that a number of frauds against government could involve collusive corruption. Economic offences and other crimes, for which there are special legislations and specialized central government agencies, are outside the purview of this guide.

Table 2

Crime	White Collar Crime	Economic Offence	Fraud	Corruption
Tax evasion	▨	▨	▨	▨
Money Laundering		▨	▨	
Bank / Insurance / Chit Fund Fraud		▨	▨	
Credit Card fraud			▨	
Bribery of Public servants				▨
Theft of cultural object		▨		
Smuggling / Illegal Foreign Trade		▨		▨
Stock Market manipulations		▨	▨	
Racketeering Travel (Passport) Documents	▨		▨	▨
Computer Crime	▨		▨	
Computer Software Piracy / Theft of Intellectual property		▨	▨	
Embezzlement / defalcation / misappropriation of money	▨		▨	
Forgery	▨		▨	
Drug Trafficking		▨		
Counterfeiting		▨	▨	
False Identity			▨	▨
Abuse of Office				▨
Theft of stores and stationery	▨			▨

3. Legal framework for dealing with fraud

Why fraud needs to be criminalized?

Fraud is not victimless. It damages the economy. Although there is no violence and no tangible visible scars, fraud generally has devastating effect on economy and society. On the economic front, fraud corrodes confidence in the financial systems (as in the Stamp Paper scam) and on the social dimension it means less money to go to the pensioner, disabled person or low-income family who really need it.

It is, therefore, necessary that the law deals with fraud as a crime and no quarter is given to perpetrators of fraud. Treating fraud as a crime has two important aspects. As a criminal offence:

- It carries a special kind of stigma (- disgrace)
- It carries a distinct range of sanctions (coercive part of the law in terms of use of force in respect of liberty or property of the convicted offender).

Attributes of a sound legal framework

Following is the essential criteria to assess the effectiveness of the legal framework in dealing with fraud:

a. ensure that effective, proportionate and dissuasive criminal, civil or administrative sanctions are available to deal with natural or legal persons;

b. designate an authority empowered to apply these sanctions;

c. sanctions should be available in relation not only to the legal persons; and

d. range of sanctions available should be broad and proportionate to the severity of a situation.

Fraud under Indian law

According to Section 17 of **Indian Contract Act** ‘Fraud’ means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto of his agent, or to induce him to enter into the contract:-

(1) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true ;

(2) the active concealment of a fact by one having knowledge or belief of the fact;

(3) a promise made without any intention of performing it;

(4) any other act fitted to deceive ;

(5) any such act or omission as the law specially declares to be fraudulent.

Fraud as defined in Section 17 of the Indian Contract Act is for the purpose of a contract and in so far as the operation of the Contract Act is concerned. In the event of a fraud, the contract becomes voidable. The party suffering from the fraud may terminate the contract on his option. The court may also compensate him if he suffers from any damage before terminating the contract. Fraud as such, is not a criminal offence. Fraud is considered a criminal offence only when it involves *impersonation, criminal breach of trust or criminal conspiracy, or forgery, or falsification or destruction of documents for wrongful gain, or embezzlement of fund.*

The Indian Penal Code

There is no separate legislation dealing with fraud as in the United Kingdom or the USA. Fraudulent activities are covered by the Indian Penal Code. The word ‘fraud’ is not defined in Indian Penal Code; instead what constitutes doing a thing fraudulently is explained. Section 25 defines the expression ‘fraudulently’ – ‘a person is said to do a thing fraudulently if he does that with intent to defraud but not otherwise’. The expression fraudulently occurs in Sections 206, 207, 208, 242, 246, 247, 252, 253, 261, 262, 263 and Sections 421 to 424.

Sections 24 and 23 define expressions ‘dishonestly’ and ‘wrongful gain and wrongful loss. ‘Wrongful gain’ is gain by unlawful means of property which the person gaining is not legally entitled. ‘Wrongful loss’ is the loss by unlawful means of property to which the person losing it is legally entitled. Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing ‘dishonestly’.

Indian Penal Code recognizes the following acts as fraud:

a. Impersonation
b. Counterfeiting
c. Wrong weighing and measurement
d. Misappropriation
e. Criminal breach of trust
f. Cheating

g. Dishonest dealing in property
h. Mischief
i. Forgery
j. Falsification
k. Possessing stolen property
l. Concealment

The Information Technology Act, 2000

India has enacted a legislation - the Information Technology Act, 2000 - to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies. The said Act also amends the related provisions in the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

The IT Act recognizes offences related to fraud such as tampering with computer source documents, hacking computer systems, creating, publishing, or otherwise making available digital signature for any fraudulent purpose.

Santhanam Committee

That there were some functional inadequacies in the IPC was recognized by the Santhanam Committee (1962) which observed that '*the Penal Code does not deal in any satisfactory manner with acts which may be described as social offences having regard to special circumstances under which they are committed and which have now become a dominant feature of certain powerful sections of modern society.'*

Santhanam Committee recommended that a new chapter be added to IPC bringing together all the offences in (such) special enactments and supplement them with provisions so that all social offences will find a prominent place in the general criminal law of the country. This recommendation was considered by the Law Commission and in its Twenty Ninth Report (1966) it observed that special enactments were of a special character and they stand apart from the general criminal law of the country embodied in the IPC and therefore 'it would be more practicable to keep provisions relating to such offences in special enactments as they are at present.'

Mitra Committee

An Experts Committee on Legal Aspects of Bank Frauds appointed by Reserve Bank of India headed by Sri NL Mitra in its report submitted in 2001 recommended that financial fraud needs to be criminalized by inserting a definition for the offence on 'financial fraud' and a penal provision in the Indian Penal Code in a new Chapter XXIV with Section 512 and 513.

Second Administrative Reforms Commission

The Second Administrative Reforms Commission in its Fourth report on Ethics in Governance made the following recommendations, including reiterating Mitra Committee recommendation, with reference to Serious Economic Offences:

a. A new law on 'Serious Economic Offences' should be enacted.

b. A Serious Economic Offence may be defined as :

   i. One which involves a sum exceeding Rs 10 crore; or

   ii. is likely to give rise to widespread public concern; or

   iii. its investigation and prosecution are likely to require highly specialized knowledge of the financial market or of the behaviour of banks or other financial institutions; or

   iv. involves significant international dimensions; or

   v. in the investigation of which there is requirement of legal, financial, investment and investigative skills to be brought together; or

   vi. which appear to be complex to the Union Government, regulators, banks, or any financial institution.

c. A Serious Frauds Office (SFO) should be set up (under the new law), to investigate and prosecute such offences. It should be attached to the Cabinet Secretariat. This office shall have powers to investigate and prosecute all such cases in Special Courts constituted for this purpose. The SFO should be staffed by experts from diverse disciplines such as the financial sector, capital and futures market, commodity markets, accountancy, direct and indirect taxation, forensic audit, investigation, criminal and company law and information technology. The SFO should have all powers of investigation as stated in the recommendation of the Mitra Committee. The existing SFIO should be subsumed in this.

d. A Serious Frauds Monitoring Committee should be constituted to oversee the investigation and prosecution of such offences. This Committee, to be headed by the Cabinet Secretary, should have the Chief Vigilance Commissioner, Home Secretary, Finance Secretary, Secretary Banking/ Financial Sector, a Deputy Governor, RBI, Secretary, Department of Company Affairs, Law Secretary, Chairman SEBI etc as members.

e. In case of involvement of any public functionary in a serious fraud, the SFO shall send a report to the Rashtriya Lokayukta and shall follow the directions given by the Rashtriya Lokayukta.

f. In all cases of serious frauds the Court shall presume the existence of mens rea of the accused, and the burden of proof regarding its non-existence, shall lie on the accused.

The Second ARC also recommended enactment of a False Claims Act on the lines of US False Claims Act, which provides for citizens and civil society groups to seek legal relief against fraudulent claims against the government. This law should have the following elements:

a. Any citizen should be able to bring a suit against any person or agency for a false claim against the government.

b. If the false claim is established in a court of law, then the person/ agency responsible shall be liable for penalty equal to five times the loss sustained by the exchequer or society.

c. The loss sustained could be monetary or non-monetary as in the form of pollution or other social costs. In case of non-monetary loss, the court would have the authority to compute the loss in monetary terms.

d. The person who brought the suit shall be suitably compensated out of the damages recovered.

Civil Service Regulations

In addition to the provision as contained in the IPC, the Union Government and the State governments formulate Rules that govern the service conditions of their employee. The most important one is the Civil Services (Conduct) Rules, which lay down the rules of behaviour for the public servants. The General Financial Rules (2005) in case of the central government and the Financial Rules of the State lays down the essential internal controls in respect of maintenance of accounts, handling of cash, procurement, etc. They also prescribe the action to be taken once a fraud or loss of government property is discovered – such as the authorities to be informed, reports to be filed, etc. The main stipulations given in the Andhra Pradesh Financial Code in respect of loss of assets though fraud are summarized below:

a. Inform the head of the office immediately when any facts indicating that defalcation or loss of public moneys, stamp, opium, stores or other movable or immovable property has occurred or that a serious account irregularity has been committed come to the notice of any government servant;

b. Report to the higher authorities losses involving embezzlement, serious irregularities etc. irrespective of amount involved;

c. Send a preliminary report the matter to the government without delay if it appears to the head of the office prima facie that there has been any such occurrence which concerns his office or in which a government servant subordinate to him is involved. These reports should be sent even when the person responsible for a loss has made it good;

d. Submit to the Accountant-General a report on the exact nature of the defalcation or loss and circumstances which made it possible.

e. Investigate the matter fully without delay and take all necessary further action;

f. Request the Accountant General to furnish all vouchers and other documents in his possession that may be relevant to the investigation.

g. Seek the services of an audit officer for the purpose if the investigation is as complex as to require the assistance of an expert audit officer.

h. Send a complete and detailed final report to the Accountant General and, through proper channel to the head of the department describing the nature and extent of the loss on account irregularity and the circumstances (including any breach or neglect of an existing rule) which made it possible and to recover it in any way as soon as the investigation is complete. *The report should also state what disciplinary action has been taken or recommended with a view to prevent the recurrence of any such loss or account irregularity*.

i. The head of the department should also submit a final report to the government giving full information on all above points and, when necessary, making his recommendations.

j. Take competent legal advice at once whenever it appears likely that judicial proceedings in connection with a loss sustained by the government are imminent.

k. Report the matter at once to the Police, as a general rule, whenever there is a reasonable suspicion that a criminal offence has been committed in respect of public money or property under intimation to the head of his department.

l. Ensure that all the witness serving in the department and all documentary evidence in the control of the department are punctually produced when the case is heard by the Court.

m. Appoint an officer of the department to attend the proceedings in the Court and assist the prosecuting staff.

n. Send a full statement of the facts of the case to higher authorities if prosecution results in the discharge or acquittal, or in the imposition of any sentence which appears to be inadequate with a request that further proceedings should be taken up for revision or appeal.

o. Submit promptly the following reports to the government through the proper channel at each stage regarding –

- The commencement of the Police investigation;
- The decision to prosecute in any particular case;
- The results of any prosecution
- The decision to proceed further in revision or appeal in any case, and
- The results of any proceedings in revision or appeal

Fraud legislation – An International perspective

Under the **Fraud Act 2006 (UK)** a person is guilty of fraud if he is in breach of any of the following:

- fraud by false representation;
- fraud by failing to disclose information; and
- fraud by abuse of position.

Fraud by false representation occurs when a person

1. dishonestly makes a false representation, and
2. intends, by making the representation to make (i) a gain for himself or another, or (ii) to cause loss to another or to expose another to a risk of loss.
    - A representation is false if it is a) untrue or misleading and b) the person making it knows that it is, or might be, untrue or misleading.
    - A representation may be express or implied

(An example of a representation by conduct is where a person dishonestly misuses a credit card to pay for items. By tendering the card, he is falsely representing that he has the authority to use it for that transaction. It is immaterial whether the merchant accepting the card for payment is deceived by the representation.)

Fraud by failing to disclose information occurs when a person

1. dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and
2. intends, by failing to disclose the information (i) to make a gain for himself or another, or (ii) to cause loss to another or to expose another to a risk of loss.

Fraud by abuse of position occurs when a person

1. occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,
2. dishonestly abuses that position, and

3. intends, by means of the abuse of that position (i) to make a gain for himself or another, or (ii) to cause loss to another or to expose another to a risk of loss.

   - A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.

The Fraud Act, 2006 of U.K. is a comprehensive law dealing with frauds and covers various other aspects also such as possession of articles for use in frauds, making or supplying articles for frauds, participating in fraudulent businesses carried out by a sole trader or a company, obtaining services dishonestly and so on.

Definition of fraud in the European Union

Fraud affecting the European Communities' financial interests is looked at from the expenditure and revenue perspective:

a. *In respect of expenditure,* any intentional act or omission relating to the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds of the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities, nondisclosure of information in violation of a specific obligation with the same effect and the misapplication of funds for purposes other than those for which they were originally granted;

b. *In respect of revenue,* any intentional act or omission relating to use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the illegal diminution of the resources of the European Communities or budgets managed by, or on behalf of, the European Communities, non-disclosure of information in violation of a specific obligation or misapplication of a legally obtained benefit with the same effect. In order to deal with financial fraud in an effective manner the Convention on the Protection of Financial Interests of the Community lays down member states must criminalize the preparation or supply of false, incorrect or incomplete statements or documents. Participation or instigation in any fraud case is also sought to be criminalized. It also states that the penalties envisaged by Member States must be proportionate, effective and dissuasive. With regard to serious fraud, that is where the pecuniary limit exceeds Euro 50,000, the Convention stipulates that Member States must lay down penalties involving the deprivation of liberty, which can give rise to extradition.

Fraud under American Law

The US has enacted the Major Fraud Act 1988 that identifies fraud in the following manner.

Whoever knowingly executes, or attempts to execute, any scheme or artifice with the intent -

- to defraud the United States; or
- to obtain money or property by means of false or fraudulent pretences, representations, or promises, in any procurement of property or services as a prime contractor with the United States or as a subcontractor or supplier on a contract in which there is a prime contract with the United States, if the value of the contract, subcontract, or any constituent part thereof, for such property or services is $1,000,000 or more . . . .

Another significant definition of fraud is observed in the False Claims Act which allows people who are not affiliated with the government to file actions against federal contractors claiming fraud against the government. The Act establishes liability when any person or entity improperly receives from or avoids payment to the Federal government. In summary, the Act prohibits:

a. Knowingly presenting, or causing to be presented to the government a false claim for payment;

b. Knowingly making, using, or causing to be made or used, a false record or statement to get a false claim paid or approved by the government;

c. Conspiring to defraud the government by getting a false claim allowed or paid;

d. Falsely certifying the type or amount of property to be used by the government;

e. Certifying receipt of property on a document without completely knowing that the information is true;

f. Knowingly buying government property from an unauthorized officer of the government, and;

g. Knowingly making, using, or causing to be made or used a false record to avoid, or decrease an obligation to pay or transmit property to the government.

For unambiguous understanding and invoking of the Act the False Claims Act also defines the words ‘**Knowing and Knowingly’.** For purposes of this section, the terms “knowing” and “knowingly” mean that a person, with respect to information -

- has actual knowledge of the information;
- acts in deliberate ignorance of the truth or falsity of the information; or
- acts in reckless disregard of the truth or falsity of the information, and
- no proof of specific intent to defraud is required.

Title 18, United States Code, section 287--the false claims statute--provides in part:

Whoever makes or presents to any person or officer in the civil, military or naval service of the United States, or to any department or agency thereof, any claim upon or against the United States, or any department or agency thereof, knowing such claim to be false, fictitious, or fraudulent, shall be imprisoned not more than five years.

Conclusion

Though the Indian Penal Code recognizes fraud as an offence, fraud is not comprehensively defined as in Fraud Act 2006, UK to cover false representations, failure to disclose information, abuse of position. The Fraud Act also carries specific provisions to deal with offences of obtaining services dishonestly and of possessing, making and supplying articles for use in frauds. Explicitly defining fraud makes it easy for the executive to effectively distinguish between fraud and corruption without each overlapping the other thus facilitating the identification and prosecution of the offenders unequivocally.

4. Institutional framework

Legal framework of laws and rules is by itself not helpful without supporting institutional framework capable of taking prompt, decisive and effective action against fraud.

Institutional framework in India

Unlike the UK where there is a Serious Fraud Office, an identified institution to deal serious economic offences of a certain magnitude, in India there are no specific institutions to deal with fraud. Although, a Serious Fraud Investing Office was set up in 2003 in the backdrop of stock market scams, failure of non-financial banking companies and phenomena of vanishing companies. The SFIO was set up on the basis of recommendations made by the Naresh Chandra Committee on Corporate Governance. Like the SFO UK, this is a multidisciplinary office under the Department of Company Affairs, Ministry of Finance, Government of India, which investigates those serious frauds referred to it under Section 235/239 of the Companies Act 1956. Other than SFIO, it is seen that the institutions established for dealing with corruption also have the responsibility of dealing with cases of fraud. In this section we look at various institutions that deal with fraud at the federal and the state level.

Public Accounts Committee

The Public Accounts Committee (PAC) is constituted every year for examination of reports submitted by the Comptroller and Auditor General of India to the Parliament. The PAC examines the appropriateness of the expenditure incurred by the government as presented in the accounts, the reported cases of losses, financial irregularities in the government, and so on. While examining the reports of the CAG, the committee also verifies the various aspects of the government's tax administration, namely cases of under-assessments, tax evasion, non-levy of taxes, etc thus identifying the loopholes in the tax laws and procedures.

Similarly, PAC of the state legislature examines the reports of the CAG on the state government's accounts and in the process also deals with cases of fraud, misappropriation, embezzlement, etc. and makes suitable recommendations to the state government.

Comptroller & Auditor General of India

Comptroller and Auditor-General is the constitutional authority charged with the responsibility of auditing all receipts and expenditure of the Union

Government and that of the States and Union Territories and agencies under them. In his capacity as the statutory auditor of the government, he has the responsibility of oversight in respect of all government transactions.

As mentioned above, the reports of Comptroller and Auditor General of India are deliberated upon by the Public Accounts Committee (PAC) and the Committee on Public Undertakings. CAG assists the above mentioned legislative committees by scrutinizing the notes which the Ministries submit to the Committees and helps the Committees to check the correctness of facts and figures in their draft reports.

At the state level, while the Chief Minister is the ultimate political authority to hear complaints against the ministers and all administrative departments of the State, the Governor has the powers to authorize the CBI to make enquiries against the ministers including the chief minister in cases of any complaints against the administration.

Chief Secretary of the State

The Chief Secretary is the highest administrative authority dealing with complaints of misconduct and fraud committed by any Department of the State. If the complainant is not satisfied with the response of the Departmental CVO or the VC, then the final administrative relief can be obtained from the Chief Secretary before seeking any legal or political relief.

Crime Investigation Department (CID)

While the local police station is the first line investigating agency for any crime, the white collar crime and larger issues like scams and frauds are dealt by the Crime Investigating Department. The CID is an integral part of the Police Department originally formed in 1903. It monitors and oversees the crime situation throughout the State, analyses the crime trends and the quality of investigations. It maintains and updates all criminal information and records, collects crime intelligence and assists the District/City Police in crime prevention and detection. It organizes study of different facets of crime by various agencies. The CID works with different wings, each dealing with individual issues of crime. One of them is the Economic Offences Wing that deals with the white collar crime, fraud, etc.

Economic Offences Wing: The wing investigates cases pertaining to misappropriation, cheating, forgery, counterfeit currency, cyber crimes and major frauds, scams and other white collar offences. The wing collects intelligence on the above categories of crime and undertakes analysis. It also liaises with other Economic Enforcement agencies like Income-Tax Department, Customs & Central Excise, Reserve Bank of India, Commercial Banks etc. in the discharge of its functions. It advises the government on the enactment of suitable acts/Laws in this sphere.

State Vigilance Commission

The Andhra Pradesh State Vigilance Commission was established in the year 1964 as an independent advisory body to deal with the prevention of corruption and maintenance of integrity in public services on the lines of Central Vigilance Commission. The Commission is essentially an independent anti-corruption oversight body to advise the government on issues of corruption and misconduct or other malpractices of the public servants in the execution of their administrative and executive powers of the State.

Under the scheme of the Vigilance Commission each Secretariat Department is required to have a Chief Vigilance Officer and similarly every Head of Departments, Government Undertaking / Government Company and such other Institutions as may be notified by the Government from time to time should have a Vigilance Officer. The District Collector of each District is supposed to function as the Chief Vigilance Officer within his jurisdiction.

The government has issued clear guidelines in Circular Memo No.235/Spl.B/2000-1, dated 26.7.2001 with regard to the nature of cases that could be referred to the Commission for advice. The circular categorized the disciplinary cases into vigilance and non-vigilance cases. Cases of misconduct on part of the public servants involving lack of integrity like illegal gratification, bribery, unlawful gain to self and others, criminal misconduct such as misappropriation and cheating are categorized into vigilance cases and are to referred to the Commission for advice. Cases of misconduct that are administrative in nature and require disciplinary action could be dealt by the individual department heads and need not be referred to the Commission. The Government vide GO Ms No 522 dated 21-07-2007 redefined the term vigilance angle as used in the vigilance manual. Accordingly the cases that can now be referred to the Commission should involve one or more of the following:

- Demanding and / or accepting gratification other than legal remuneration in respect of an official act or for using his influence with any other official.
- Obtaining valuable thing, without consideration or with inadequate consideration from a person with whom he has or likely to have official dealings or his subordinates have official dealings or where he can exert influence.
- Obtaining for himself or for any other person any valuable thing or pecuniary advantage by corrupt or illegal means or by abusing his position as a public servant.
- Possession of assets disproportionate to his known sources of income.

- *Cases of misappropriation, forgery or cheating or other similar criminal offences.*
- Other irregularities where circumstances will have to be weighed carefully to take a view whether the officer's integrity is in doubt, Gross or willful negligence, recklessness in decision making, blatant violations of systems and procedures; exercise of discretion in excess, where no ostensible / public interest is evident; failure to keep the controlling authority / superiors informed in time.
- Any undue / unjustified delay in the disposal of a case perceived after considering all relevant factors, would reinforce a conclusion as to the presence of Vigilance angle in a case.

As can be seen, the Vigilance Commission is entrusted with the responsibility of examining cases of misappropriation, forgery or cheating or other similar criminal offences.

Directorate General (Vigilance & Enforcement)

The Directorate General of Vigilance and Enforcement is a comparatively new and a unique enforcement agency with enforcement powers in respect of a number of departments like taxation, transport, mining, etc. It was set up through an executive order in June 1985 as part of the General Administration Department under an Additional Director General of Police with ex officio status of Principal Secretary to government to conduct enquiries or investigations into specific allegations affecting public interest; and to take effective measures on its own and with the help of other vigilance bodies, organisations and departments of government to prevent leakage of revenues, detect misuse or wastage of government funds and resources, prevent of loss of State's wealth and natural resources; and losses, wastage and graft in public sector undertaking and government companies. It is also authorized to advise government regarding changes that may be made in laws and rules to achieve the above purposes and on matters that may be referred to it. It is also to carry out vigilance functions where government spending or enforcement functions in respect of revenues due to government is involved. It discharges its functions through four wings viz. revenue, engineering, development works and natural resources with 12 regional offices. The department has State-wide jurisdiction in respect of matters to which the executive authority of the State extends covering all departments of government, State public undertakings, State government companies, all local bodies and other institutions and organizations receiving assistance from the government.

At the instance of the Vigilance Commission, the Directorate General of Vigilance and Enforcement has been re-vested with powers of police officers under clauses (o) and (s) of section 2 of Criminal Procedure Code to investigate corruption and criminal offences which come to notice in the course of discharge of its functions. The references made by the Vigilance Commissioner, the institution of Lokayuktha and Upa lokayuktha and the Chief Minister Secretariat and the Chief Secretary are enquired into or investigated by the Directorate General. The reports of the Directorate General of Vigilance and Enforcement having a vigilance angle are now required to be sent to government through the Vigilance Commission with his advice. Departments are required to take action on the enquiry reports and where vigilance aspect is involved to take into account the advice of the Vigilance Commission.

Lokayuktha & Upa Lokayuktha

In the wake of recommendations of the first Administrative Reforms Commission many State governments had enacted the Lokayuktha Act to investigate and report on allegations or grievances arising out of the conduct of public servants including *political executives*, *legislators*, officers of the State government, local bodies, public enterprises and other instrumentalities of government including cooperative societies and universities. By virtue of this Act any member of the public can file specific allegations with the institution against public servants which will be enquired into by the Lokayuktha subject to merits of the allegation. It is also open to the Lokayuktha to initiate suo moto inquiry into conduct of public servants. Though the Lok ayuktha came into existence at the time the Vigilance Commission ceased to function, even after the revival of the VC, the Lok Ayuktha continues to function. Matters for the investigation by the Lok Ayuktha can be brought to its notice by:

- Complaint by the aggrieved person.
- Based on the information received otherwise than by way of complaint like newspapers, reports, etc.
- Reference from the Governor.

The institution has its own investigating section consisting of Senior Police officers to investigate into the complaints including the suo moto references pertaining to serious allegations and confidential enquiries. There is also a legal section headed by a person of the rank of a district judge that will examine the preliminary investigation reports submitted by the various investigating agencies including the investigating section of the aforesaid institution and prepares their report to be submitted to the Lokayukta or Upa Lokayukta. If the lokayuktha or upa lokayuktha finds that the allegations against the public servant have been substantiated, it recommends to the competent authority of the appropriate action and the competent authority shall take action within 3 months from the date of receipt of the report. In case, the lok ayuktha recommends the imposition of penalty of removal from office of the public servant, the competent authority shall without further enquiry take the action. Thus, the objective with which the Andhra Pradesh State Legislature passed the Andhra Pradesh Lokayukta and Upa Lokayukta Act, 1983 is that the Institution established under the Act should provide easy and cost free access to the common people, redress their grievances speedily and effectively in the process of checking and mitigating corruption and maladministration.

However, as can be observed, the lok ayuktha and upa lok ayuktha deal with matters that fall under the definition of corruption and have little role to play on matters concerned with fraud.

Anti Corruption Bureau

Established in the year 1961, the Anti-Corruption Bureau is a specialized agency tackling the problem of corruption in various departments of the government against public servants and against private persons by the public servants. The Bureau basically enforces the provisions of the Prevention of Corruption Act 1988. In addition to this, the ACB also conducts enquiries based on the petitions received from other agencies like government, Vigilance Commission, Lokayuktha etc. The ACB conducts searches and surprise inspections to unearth corrupt practices and disproportionate assets.

It also

- undertakes surprise inspections of offices;
- verifies possession of unauthorized cash by public servants, presumed to be bribes paid to public servants, while on duty at the office;
- conducts raids on check-posts run by departments;
- undertakes verification of attendance of officers particularly in basic service departments like primary health centres;
- verifies stocks of drugs and tallies stock accounts;
- verifies stores and stationery in public offices etc.

It is competent to conduct investigations not only against government servants but also other public servants who are employees of various State public sector undertakings, statutory corporations, government companies and local authorities. All reports of the ACB are sent to the concerned department in the Secretariat through the Vigilance Commission who in turn forwards it to the department concerned with his recommendation.

Conclusion

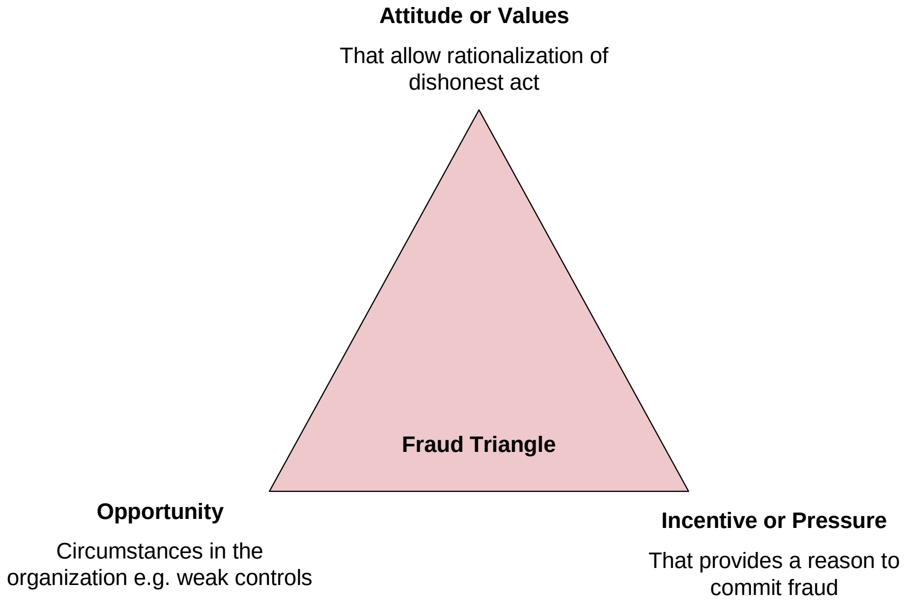
As mentioned in the beginning of this section, there is no dedicated institution to deal with cases of fraud. The institutions which have been established viz. Vigilance Commission, Director Vigilance and Enforcement, etc. to deal with corruption also deal with fraud in government. On the whole, the institutional framework for dealing with frauds is adequate in terms of coverage. However, it has been observed by the field officers that both the CID and ACB lack expertise in dealing with serious frauds having complex accounting or legal operations. This is one area that requires strengthening.

5. Good Practices

‘Fraud is any intentional act or omission designed to deceive others and resulting in the victim suffering a loss and / or the perpetrator achieving a gain.’

Managing the Business Risk of Fraud: A Practical Guide (Exposure Draft), Institute of Internal Auditors

Typically, fraud takes place when there is a) an *incentive* (low risk - high return) or *pressure* (of personal circumstances, say indebtedness or an addiction); and b) an *opportunity* present in the form of a weak control (an open door); and c) an *attitude* or *value* which allows the perpetrator to rationalize the fraudulent act (e.g. it is their mistake that they left the door open; or they deserve / can afford it anyway). The Fraud Triangle[5] (see figure below) is key to understanding and dealing with the risk of fraud as all measures for mitigating the risk have to deal with tackling these three elements one way or the other. If strong and effective internal controls deny the opportunity for fraud, equally strong detect controls would take away the incentive for committing fraud.


Attitude or Values
That allow rationalization of dishonest act
Fraud Triangle
Opportunity
Circumstances in the organization e.g. weak controls
Incentive or Pressure
That provides a reason to commit fraud

[5] Tackling Staff Fraud and Dishonesty: Managing and Mitigating Risks – CIPD Guide

The Good Practices have been grouped under the following four broad headings:

A. *Deterring Fraud;*

B. *Preventing Fraud that could not be deterred;*

C. *Detecting Fraud that could not be prevented; and*

D. *Investigating and dealing with frauds detected.*

Some of the 29 good practices given in the following sections are possibly being practiced to some extent in some departments already. Traditionally, anti-fraud measures are more commonplace in revenue departments than in expenditure departments. Practices such as publicity campaigns (creating anti-fraud culture and awareness) have been extensively used by Income Tax and Central Excise departments. Some practices (e.g. data mining and data matching) presuppose existence of data in digitized form. Such practices will have to wait till the right environment is created. Considering the increasing use of computers in government, it is only a matter of time before these practices would also become practical propositions. Increasing use of computers brings in its wake increased fraud risks along with the benefit of speed and ease in carrying out various transactions. The recommended good practices lay due emphasis on dealing with them, even though they may seem not so relevant to government sector today.

A: Deterring Fraud

'All types of fraudsters weigh up the potential gains against the risk of getting caught and the sanctions they may face. Government departments and agencies need to make fraud as unattractive as they can'

Good Practice in Tackling External Fraud –
National Audit Office
& HM Treasury, U.K.

The objective of deterrence is to ensure that the totality of anti-fraud measures represent the strongest deterrent possible to those perpetrating or considering perpetrating fraud. Deterrence in practice is achieved when an organization puts in place strong measures of

- prevention;
- detection;
- sanction; and
- financial redress (recovery)

These measures should be effectively publicized and communicated.

The most effective method of countering fraud is deterring the fraudster from committing the fraud. Fear is the greatest deterrent. Criminalization of fraud combined with stringent penalties acts as a deterrent. On the other hand, poor detect controls and ineffective investigation convinces the fraudster that he/she can get away with the crime. The organization should ensure that opportunities for fraud are minimized and the potential fraudster does not find it easy to defraud. In other words, the message that potential fraudsters should get is that:

- strong controls exist that will stop them from succeeding;
- even if they do manage to commit the fraud, evidence of their fraud will be discovered sooner than later and they will be most likely caught;
- they will face stiff penalties; and
- amount gained from fraud will be recovered.

All fraud control measures, if effective, would deter fraud. For example, the near certainty / high probability of fraud being found out eventually (detect measures) would deter a potential fraudster. Similarly, a professional and competent investigating system coupled with speedy conviction and punishment would discourage a potential fraudster from committing fraud. Legally backed and sound measures to recover the money gained through fraud would make the fraud unattractive and thus act as a deterrent. However, there are some overarching and general measures that could be considered essentially deterrent in their nature. To illustrate, having a fraud control policy, creating public awareness, having a fraud response plan and so on could be considered clearly deterrent measures.

In a sense, all fraud control measures are aimed at deterring fraud. Strong prevent controls will deter fraud as do strong detect controls. Any classification of fraud control measures is subjective and there is no hard and fast rule that it should be one way rather than another.

Given below are some questions that a department / agency might like to ask itself to check if the deterrent practices are adequate.

Check List of questions

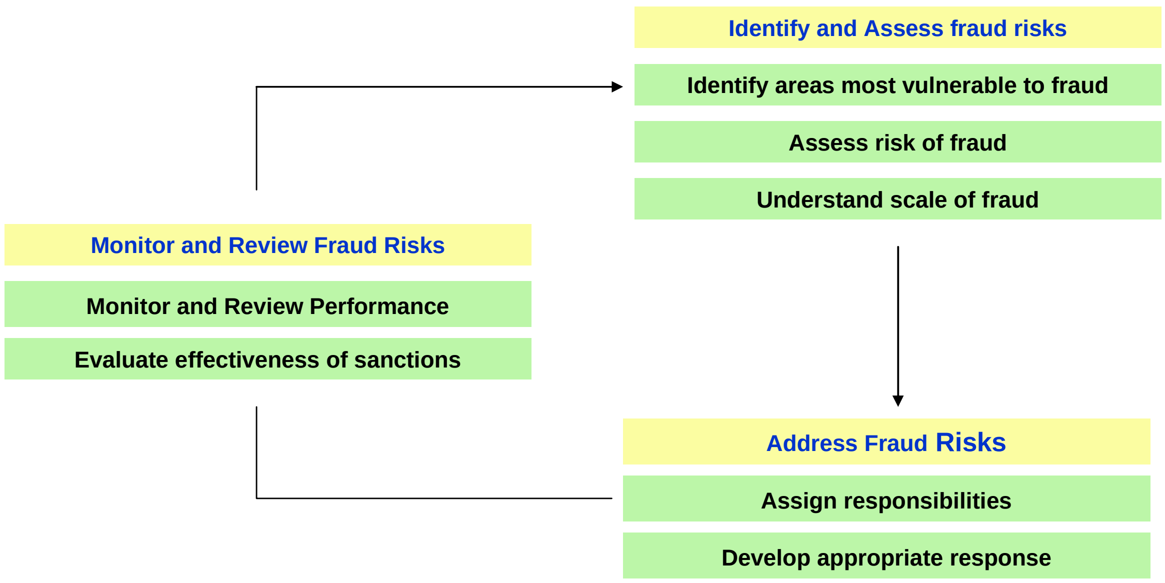
Does your organisation:

- seek to influence employees', customers' and the wider general public's attitude to fraud;
- send a strong message to potential fraudsters that they are likely to be caught and sanctions will be imposed. For example, are there press releases on employees / businesses prosecuted and are there any targeted or wider campaigns regionally or nationally?
- have an anti-fraud culture where staff understand the standards of conduct required and their personal responsibilities in preventing fraud, applying controls and reporting cases of suspected fraud.

A.1. Adopt a Strategic and Risk-based Approach to Managing Fraud

In the absence of a strategic approach, fraud will be dealt with as and when it takes place. That is, there is no effort to pro-actively deal with fraud risk. On the other hand, a strategic approach to tackling fraud takes a holistic approach of integrating systematically the risk assessment and management at the organization and the operational levels.

Main elements of strategic approach to dealing with Fraud


Identify and Assess fraud risks
Identify areas most vulnerable to fraud
Assess risk of fraud
Understand scale of fraud
Monitor and Review Fraud Risks
Monitor and Review Performance
Evaluate effectiveness of sanctions
Address Fraud Risks
Assign responsibilities
Develop appropriate response

While the strategic approach aims at adopting a holistic view of tackling fraud, the risk-based approach enables the organization to target its resources at the problem areas. The basic difference between the strategic approach and the risk based approach is that in the former assessment of the risk of fraud is more broad based while the latter identifies the problem areas and responds to each vulnerable area. The risk based approach involves the following:

a. Assessing the organization's vulnerability to fraud;

b. Identifying the areas most vulnerable to risk of fraud;

c. Evaluating the scale of fraud risk;

d. Assigning ownership;

e. Preparing response to the risk of fraud; and

f. Measuring the effectiveness of fraud-risk strategy.

An organization would be said to have adopted a strategic and risk based approach to tackling fraud, if it does the following:

√ Assesses the size of the threat from fraud and, where significant, undertake a separate fraud risk assessment.

√ Identifies the areas most vulnerable to the risk of fraud.

√ Finds out the

  - size of the fraud threat
  - types of fraud committed
  - who is committing them
  - how often
  - how much is involved

√ Has a package of measures in place to tackle losses from fraud where these are significant.

√ Has targets to stabilise or reduce fraud.

√ Allocates responsibilities for tackling fraud risks to ensure that risks are managed, plans are implemented and progress monitored.

This good practice actually involves having in place or practicing other good practices. This is more an approach and a guiding philosophy adopted and owned by the top management to tackle fraud in the organization. It is this practice which gives coherence and structure to other fraud control measures.

A.2. Create an anti-fraud culture through publicity campaigns

Anti-fraud culture implies that those within the organization and those stakeholders outside it are sensitized about the implications of fraud on their work and lives. For example, fraud in construction of a bridge can have serious implication to the safety of its users. Similarly, frauds involving medical supplies in a government dispensary could have grave consequences for general public accessing that service. Also, the more government resources are lost to fraud, the less will be available for public service delivery. Thus, it is important that the general public is made aware of the part that they can play in fraud control through publicity campaigns. The public must be informed of avenues for reporting fraud and assured that they can report their suspicions in the strictest confidence. It is also important to communicate to external stakeholders because there are strong community expectations upon government organizations that the public monies they control are well protected against misuse and loss. The community has a right to expect that government departments and agencies have taken all reasonable and cost effective measures to prevent and detect losses due to fraud.

Anti-fraud culture would also require that potential fraudsters are forewarned of the consequences of fraud. A potential fraudster is deterred by the prospect of being caught and strict action that would follow. A fraudster takes time to identify the opportunities, calculate the risks and rewards and determine whether the risk is worth taking. As part of these calculations, the potential fraudster would also consider the likely consequences of an investigation. Therefore, if the detect measures are seen to be good and sanctions in case of detection are severe and prompt, a potential fraudster would think twice before committing a fraud. The aim of creating an anti-fraud culture is to create this aura about the organization that frauds are more likely to be detected than otherwise and that investigation is quick and punishment commensurate with size and nature of fraud.

Ideally, the head of the organization should have a statement issued from her / his desk that the department has anti-fraud mechanism in place. This shall be stated at all prominent places of office and correspondence with external parties and also appear on the website of the department.

Illustration

The main message of the U.K. Department for Work and Pensions' Targeting Fraud campaign was to show that cheats get caught and punished.

For their campaign between September 2001 and March 2002 the Department developed television, radio, press and poster advertisements to show that cheats get caught and punished. The main messages were:

Fraud will be punished - Fraud is a crime, and benefit cheats do get caught. And new penalties and support for prosecutions means that the punishments for fraud can be very serious.

The Department for Work and Pensions are cracking down on fraud - Through new measures for prevention and more efficient detection, fraud will become increasingly more difficult to commit and to conceal – cheats do get caught.

Fraud has victims - Benefit fraud is at everyone's expense. Benefit cheats are stealing money from people who need it. And they are stealing money from every taxpayer. Fraud is not a victimless crime and it adds up.

Benefit fraud - We aim to put a stop to it.

Benefit fraud - We're on to you.

Source: Department for Work and Pensions, U.K.

A.3. Create awareness about fraud risk among employees

‘Almost every time a major fraud occurs many people who were unwittingly close to it are shocked that they were unaware of what was happening. Therefore, it is important to raise awareness through a formal education and training programme as part of the overall risk management strategy. Particular attention should be paid to those managers and staff operating in high-risk areas, such as procurement and bill paying, and to those with a role in the prevention and detection of fraud, for example human resources and staff with investigation responsibility.

‘There are arguments about how far training on fraud should go within an organisation beyond the audit group – for example a question often raised is whether management and staff who have been trained in fraud prevention techniques will then use the knowledge to commit fraud. However, there is advantage in covering the subject of fraud in generic terms, the corporate ethic, the audit approach and the types of checks and balances built into processes.’

Fraud Risk Management – A Guide o Good Practice
Chartered Institute of Management Accountants, U.K.

It is recommended that the organization conduct campaigns and training programmes aimed at the employees, citizens and third party providers to create awareness about its anti-fraud policy. New employees should be similarly informed at the time of induction training. The campaign / training should cover a) employees’ duty to communicate actual or suspected fraud along with specific examples; and b) information on how to communicate such matters.

Fraud awareness program should cover the following topics:

- the damage that fraud causes to the economy, effective delivery of services to citizens, public confidence in institutions and so on;
- what constitutes fraud—with suitable examples to illustrate the fact that it can involve tangible and intangible assets;
- the need for ethical behaviour and the fact that fraud control is everyone’s responsibility;
- the organization’s fraud policy statement and control plan, and any procedures and manuals regarding fraud;
- things (red flags) to look out for that may indicate a fraud has been committed;
- what to do if fraud is suspected;
- who is responsible for handling allegations and cases of fraud (and breaches of the Conduct Rules); and
- remedies that are available to be applied when fraud or misconduct are established.

A.4. Issue a Fraud Risk Control Policy

The Government should adopt a fraud risk control policy, which could form part of the State's Financial Code. Each Department and organizations under it could thereafter have their own Fraud Risk Control Policy which may be adopted to suit their specific circumstances and nature of activities. For instance, Department of Health, Commercial taxes Department, Road Transport Authority, etc. could have their own specific Departmental / Organizational Fraud Control Policies under the over all government policy.

A Fraud Risk Control Policy should

a. spell out clearly how the organization views fraud and how it intends to deal with it;

b. set out guiding principles and the broad arrangements for effectively tackling the risk of fraud;

c. send a strong signal that the organization takes the issue of fraud seriously, that is, it has a zero tolerance attitude towards fraud; and

d. provide an assurance that it has in place suitable measures in place to deal with it.

Given below is the suggested framework for Fraud Risk Control Policy

1. Introduction

Policy statement
Scope of policy
What constitutes a fraud?
Statement of attitude to fraud
Code of conduct
Conflict of interest policy

2. Summary of Fraud Control Strategies

Appointment of fraud control officer / counter fraud unit (if any)
Fraud control responsibilities
Fraud risk management (including fraud risk assessment)
Fraud awareness
Fraud detection
Fraud reporting
Investigation of fraud and other improper conduct
Internal control review following discovery of fraud
Internal audit program

3. Fraud Risk Management

Regular program for fraud risk assessment

Ongoing review of fraud control strategies

Fraud risk assessment

Implementation of proposed actions

4. Procedures for Reporting Fraud

Internal reporting

Reports by members of staff

External anonymous reporting

Protection of those reporting suspected fraud

Reports to the police

Reports to external parties

5. Procedures for Fraud Investigation

Internal investigations

External investigative resources

Documentation of the results of the investigation

Recovery of amounts gained through fraud

A sample policy is given in Appendix A at the end of this section for guidance.

A.5. Develop a 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 is taken to:

a. Prevent further losses of funds or assets where fraud has occurred and to maximise recovery of losses;

b. Minimise the occurrence of fraud by taking rapid action at the first signs of a problem;

c. Maximise the success of any disciplinary/legal action taken by securing evidence
   - without alerting suspects at the outset of the investigation; and
   - in a legally admissible form;

d. Minimise any adverse publicity and dislocation suffered as a result of fraud;

e. Identify lessons which can be used as a guide in managing fraud in future;

A suggested outline Fraud Response Plan is given below:

1. Purpose of the Fraud Response Plan (a-e above)

2. Roles and Responsibilities of:
   - Managers and supervisors
   - Fraud Control officer (if any)
   - Human resources section
   - Internal auditors
   - External auditors
   - Legal advisors
   - IS/IT staff
   - Public relations
   - The police

3. Possible courses of action with respect to fraud
   - Disciplinary action
   - Civil response
   - Criminal response

- Parallel response

4. The Response

- Establish an inquiry officer / team

5. The Investigation

- Preservation of evidence
- Physical evidence
- Interviews (general)
- Statements from witnesses
- Statements from suspects

6. Follow up Action

- Lessons learned
- Management response

A fraud response plan applicable for all departments can be part of the State's Financial Code.

A.6. Develop and communicate to all employees a uniform code of conduct

Counter-fraud strategy is not just about preventing fraud from being perpetrated but it should also address the attitudinal change in the employees. Every employee needs to know what behavior is expected and acceptable and what is not acceptable. The employees should sign a statement of acceptance of the code of conduct at the time of their induction into employment. The code shall address the process of fair dealing in external transactions, protection and proper use of the organization's assets, confidentiality of information, compliance with laws, rules and regulations, etc.

Conflict of Interest

The issue of conflict of interest—the conflict between one's private and public interests, is a matter that concerns everyone in public service. Management and other employees need to be conscious of any possible conflict of their personal interest with their official responsibilities. They should have means and procedures to declare that interest and have it appropriately addressed. Contracts and Memoranda of Understanding with external providers should include provisions and/or clauses covering conflict of interest. Similarly, members of tender committees, selection committees and Departmental Promotion Committees should be required to declare that he/she has no interest in any of the parties / candidates under consideration.

The Second Administrative Reforms Commission recommended that:

- 'Public Service Values' towards which all public servants should aspire, should be defined and made applicable to all tiers of Government and parastatal organizations. Any transgression of these values should be treated as misconduct, inviting punishment.
- Conflict of interests should be comprehensively covered in the code of ethics and in the code of conduct for officers. Also, serving officials should not be nominated on the Boards of Public undertakings. This will, however, not apply to non-profit public institutions and advisory bodies.

A.7. *Assess the organization's vulnerability to fraud and identify and earmark those areas that are most vulnerable to risk of fraud*

The first step in managing risk of fraud is to acknowledge the vulnerability or exposure of the organization to the risk of fraud. For example, the Social Welfare Department would need to recognize that the funds it sanctions under various schemes for the welfare of students from the weaker section could be subject to fraud because the 'beneficiaries' may manipulate certificates in order to receive benefits.

First of all, the organization must get a clear picture of its fraud risk profile by

- listing all its activities;
- assessing each activity for the likelihood of a fraud being committed; and
- estimating likely extent of damage or loss that would be involved.

Each area should be assessed in terms of particular forms of threat such as

- Theft;
- Misappropriation of funds or assets;
- Fraudulent administration of contracts; and falsification of source records for improper advantage. (Appendix B given at the end of this section lists fraud risks in different areas.)

This would provide a fair idea of fraud risk and the weaknesses in the activities that need to be addressed. This is a prerequisite for addressing the threats.

An organisation which has not previously identified its risks in a structured way, or a newly formed organisation, or a new project or activity within an organisation should assess the risks in a systematic manner as detailed above. Thereafter, it should continuously and routinely carry out risk assessment to identify new risks which did not previously arise, changes in existing risks, or risks which did exist but are no longer relevant to the organisation. The Departments have to undertake additional risk assessment whenever there is:

- Change in the environment in which organization is working
- New legislation requiring improvement in controls
- Developments in technology
- Identified weaknesses pointed out by Internal auditor

Various techniques are applied for identifying the processes or activities at risk of fraud:

- Process mapping through brain storming sessions, interviews, facilitated workshops and discussions
- Benchmarking with organizations in similar activity
- Assessing and ranking the vulnerability in each area and activity.

Fraud, by definition, entails intentional misconduct, designed to evade detection. As such, the fraud risk assessment team should engage in strategic reasoning to predict the behavior of a potential fraud perpetrator. Strategic reasoning requires a skeptical mind-set and involves asking questions such as:

- √ How might a fraud perpetrator exploit weaknesses in the system of controls?
- √ How could a perpetrator override or circumvent controls?
- √ What could a perpetrator do to conceal the risk of fraud?

Strategic reasoning is also important in designing fraud-detection procedures that a perpetrator may not anticipate. A fraud and misconduct risk assessment generally includes the following three elements:

Identify inherent fraud risk[6]

The department / agency should first of all gather information to obtain the population of fraud risks that could apply to the organization. Included in this process is the explicit consideration of all types of fraud; incentives, pressures, and opportunities to commit fraud; and IT fraud risks specific to the organization.

It is important to recognize that there are a) opportunist frauds committed by individuals who attempt to increase the amount of benefit they receive or decrease the amount paid as tax by providing false information or concealing true circumstances or facts; and b) systematic or organized frauds (involving stolen, altered or counterfeit instruments of payment, or through creation of fictitious identities such as ghost employees, ghost beneficiaries, etc.).

Assess likelihood and significance of inherent fraud risk

Assessing the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with business process owners.

Respond to likely and significant fraud risks

The department / organization should decide the specific response to address the identified risks. It should preferably carry out a cost benefit analysis of implementing controls or specific fraud-detection procedures. It should apply

[6] Inherent risk is the risk that exists before applying controls

a framework to document the fraud risk assessment, beginning with a list of identified fraud risks, which are then assessed for relative significance and likelihood of occurrence. The team should then map the risks to relevant controls, which are evaluated for design effectiveness and tested to validate operating effectiveness. Next, the organization should develop a response to residual fraud risks. The following framework illustrates how the elements of fraud risk identification, assessment, and response are applied in a rational, structured approach.

Fraud Risks identified	***Likelihood***	***Significance***	***People/ Depart-ment***	***Anti-fraud controls***	***Assess effectiveness of controls***	***Residual Risk***	***Fraud Risk Response***
Risk 1							
Risk 2							
Risk 3							

Assessing the likelihood and significance of each potential fraud risk is a subjective process. All fraud risks are not equally likely, nor will all frauds have a significant impact on the organization. Assessing likelihood and significance allows the organization to manage its fraud risks and apply preventive and detective procedures rationally.

Likelihood

Assessment of the likelihood of a fraud risk occurring is informed by instances of that particular fraud occurring in the past, the prevalence of the fraud risk in that particular activity, the organization’s overall control environment, and other factors, including the number of individual transactions, the complexity of the risk, and the number of people involved in reviewing or approving the process. Organizations can categorize the likelihood of frauds occurring in as many categories as necessary, but three categories are generally adequate: remote, reasonably possible, and probable.

Significance

The assessment of the significance of a fraud risk should include besides monetary impact, significance to an organization’s operations, reputation, as well as criminal, civil, and regulatory liability. Organizations can categorize the significance of potential frauds in as many categories as necessary, but three categories are generally adequate: inconsequential, significant, and material.

People/department

As part of the risk assessment process, the organization will have evaluated the incentives and pressures on individuals and departments, and should use the information gained in that process to assess which individuals or departments are most likely to have incentive to commit a fraudulent act, and if so, through what means. This information can be summarized into the fraud risk assessment grid and can help the organization design appropriate risk responses, if necessary.

However, not all frauds can be anticipated. Sometimes people see an opportunity for fraud that nobody else has noticed. These opportunities may not be identified or anticipated in fraud risk assessment. So organisations need secondary measures for monitoring their activities. These secondary measures should involve monitoring trends, activities, complaints and compliments for signs of irregularities.

For example, an increase in the frequency of breakdown of motor vehicles or other plant may indicate that:

- Maintenance is being paid for but not performed
- Equipment is being used for additional unauthorised work
- Unqualified operators are being used
- Additional equipment apparently being hired is not being used.

An effective assessment of fraud risk identification process includes an assessment of the incentives, pressures, and opportunities to commit fraud. Fraud risk assessment should consider the potential override of controls by management as well as areas where controls are weak or there is a lack of segregation of duties.

Integrate fraud risk assessment with overall risk assessment

It is important that fraud risks are considered in the broader context of overall risk so that fraud risk assessment takes into account department-wide strategic planning. Fraud risk should not be looked at in isolation from the general activities of the department.

A.8. Assign ownership and responsibility for overall management of anti-fraud activities

An entity's organizational structure provides the framework within which its activities for achieving its objectives are planned, executed, controlled and monitored. Significant aspects of an organizational structure include defining key areas of responsibility and establishing appropriate lines of reporting.

Asian Organization of Supreme Audit Institutions (*ASOSAI)*

To help ensure that fraud and misconduct controls remain effective and in line with governmental standards, responsibility for the organization's fraud and misconduct risk management approach should be shared at senior levels (i.e., individuals with substantial control or a substantial role in policy-making).

Advisory, KPMG Forensic
(Fraud Risk Management – Developing a Strategy for Prevention, Detection and Response)

The responsibility for tackling fraud managing risks should start at the top of the organization. Although the Secretary, Head of Department or CEO of an organization is personally accountable for his/her organisation and its risk management, he must ensure that there is a framework of senior level delegation to ensure that the responsibility and authority for implementing control actions is clear. A mechanism for reporting on risk issues should be established.

Although everybody in the organization has a role to play in tackling fraud, large departments should set up a central unit with responsibility for tackling fraud. The central unit shall coordinate work on developing the department's strategies, ensuring their implementation, monitoring results and providing advice and guidance. The central unit should have teams of professionally trained investigators or enforcement officers dedicated to investigating cases of fraud. The head of the department shall have responsibility of advising, guiding and setting and monitoring of appropriate standards.

In case of smaller departments and agencies, head of the organization need to ensure that someone is fully responsible for implementing the plans for tackling fraud in the way intended and that sufficient resources are in place.

Oversight - Top Management and Internal Audit

The Chief Secretary with the assistance of Principal Secretaries (Finance) and (General Administration) / CEO should take overall responsibility for overseeing that appropriate practices in respect of managing risk are being followed at all levels in the government. CS / CEO must assess the effectiveness of the risk mitigation undertaken by the government once a year by obtaining a report on occurrence of fraud over the past year and initiate suitable remedial measures to strengthen anti-fraud measures. The Finance / General Administration Department should be designated as nodal department for assisting CS in his oversight function. Administrative Head (Principal Secretary to Government) / Head of the Department should similarly oversee the antifraud activities of the department.

The role of internal audit is to deliver an opinion to the Chief Secretary / Secretary / CEO 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 risk.

Management has the responsibility of conducting fraud investigations but internal audit may be asked to assist, and in some organisations may have 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.

Policy, Plan and Direction - Senior Management

Head of Department (Chief Controlling Officer) should be allocated the responsibility of actually carrying out the anti-fraud activities such as risk assessment, selection of suitable risk mitigation plans, their implementation and monitoring. Their specific responsibilities, which can be formally delegated, will depend to some extent on the level of fraud risk the organisation is exposed to but should include some or all of the following:

a. Develop a fraud risk profile and undertake an annual review of the fraud risks associated with each of the key organisational objectives in order to keep the profile current;

b. Establish an effective anti-fraud policy and fraud response plan, commensurate with the level of fraud risk identified in the fraud risk profile;

c. Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;

d. Establish appropriate mechanisms for:

    - reporting fraud risk issues; and

- reporting significant incidents of fraud to the Secretary;

e. Make sure that all staff are aware of the organisation's anti-fraud policy and know what their responsibilities are in relation to combating fraud;

f. Ensure that appropriate anti-fraud training and development opportunities are available to staff in order to meet the defined competency levels;

g. Ensure that vigorous and prompt investigations are carried out if fraud occurs;

h. Take appropriate legal and/or disciplinary action against perpetrators of fraud;

i. Take appropriate action to recover assets;

j. Ensure that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Implementation - Middle Management and Individual Staff Members

Head of Office should ensure that the internal controls instituted to minimize / eliminate risk of fraud are actually followed in his office. Outside of any more formal delegation of the above duties, Head of office should be responsible for:

a. Implementing and maintaining effective controls to prevent fraud commensurate with the fraud risk profile, and

b. Ensuring compliance with anti-fraud policies and fraud response plan.

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

a. Acting with propriety in the use of official resources and in the handling and use of corporate funds whether they are involved with cash or payments systems, receipts or dealing with contractors or suppliers;

b. 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.

A.9. *Estimate the scale of likely fraud, evaluate the sufficiency of the internal controls and design the counter-fraud strategy.*

'You cannot control what you do not measure'

It is important that the organization has an estimate of the extent of its exposure to fraud. While estimating the extent of fraud that the Department is exposed to, an analysis of the internal controls that are in place and their sufficiency in countering fraud is also made to assess the response of the Department to fraud.

Approach to measuring fraud

Several methods can be employed by the department for measuring fraud. Random enquiry programs may be used to provide estimates of non-compliance and facilitate research into understanding risks of fraud. *Comparison of distinct data sets* is another technique where compliance data is matched with estimates of economic activity to assess amount of fraud e.g. corporate self-assessment payments may be compared with reported profits by the companies; or data on sale of motor vehicles from dealers could be compared with vehicles registration data of the Road Transport Authority. *Statistical modeling techniques* are useful to quantify losses arising out of fraud. This involves comparing levels of actual receipts or expenditure with the total level of receipts or expenditure that might be expected using other sources of data. U.K. Customs and Excise produces an estimate of losses on VAT by comparing the total level of expenditure in the economy that is theoretically liable for VAT and the actual receipts of VAT, assuming the difference represents total revenue loss. The theoretical tax liability is worked out based on data from National Statistics Office.

Sampling is another technique to assess the scale of fraud that a department is exposed to. A representative sample of the cases is collected and the estimates of losses are generated by extrapolating the results of the sample. Driver and Vehicle Licensing Agency of U.K. uses periodic roadside surveys to assess the loss due to evasion. The disadvantage of sampling is that of precision. To achieve greater precision of results the sample size has to be substantially increased which increases the cost of estimation. For some departments it would be sufficient if a single estimate is produced while some line departments it is necessary that specific region wise or time bound estimates are produced.

Cost of Estimating Fraud

Cost involved in estimating fraud should be given due consideration in estimating fraud. The costs of measurement vary according to:

- frequency of the estimating exercise;

- sample sizes checked;
- work involved in checking each case sampled; and
- work involved in validating the results.

In case of bigger organizations, where cost of estimation justifies benefits, estimation of fraud may be continuous exercise. While this involves greatest cost, estimation can track changes and types of frauds committed. Smaller departments and agencies may not adopt continuous estimation method. Their estimates may be produced at various intervals. Although the results may be less reliable, it will indicate level of fraud which may prompt further work to be carried out. Alternatively, costs can be spread over several years by carrying out a rolling programme of estimates.

The idea of estimating fraud is also to develop a counter fraud strategy by revisiting the existing controls. If the estimation shows significant losses due to fraud, the organization will do well to do an in-depth evaluation of controls and put in place strengthened control measures.

A.10 Focus the resources on most effective anti-fraud measures

In deciding which measures to use and the extent to which to use them department or agency may assess the savings that could be achieved by targeting their resources in a better way. Savings could arise in three ways:

- The preventive effect, through improved future compliance from those previously detected committing fraud. For example, VAT yield will increase immediately from traders previously detected committing VAT fraud, but this additional yield will gradually reduce if no further checks are subsequently made;
- The deterrent effects on others that alerts fraudsters as they learn of the greater efforts being taken to crack down on fraud.
- The direct effects from recovering amounts defrauded.

Where new measures are proposed, it is good practice to pilot these beforehand to test and refine their operation, assess their likely effectiveness and the type of savings that can be achieved.

A.11. Work together for tackling fraud.

Fraud in the Government is not an isolated issue plaguing one department or one field of activity. This is common to most Departments and it effects the overall functioning of the Government. Not only should all the Departments of the state government cooperate with each other but they should also enlist cooperation of central agencies to tackle this burgeoning problem. Departments should conduct joint training programs for their employees for creating awareness on the anti-fraud measures adopted by the Government.

Joint working enables departments to identify common threats and pool their knowledge and expertise to investigate fraudsters. Other benefits of working together to tackle fraud are:

- Good practice can be shared across departments;
- Information can be exchanged more efficiently;
- Skills, informal systems and culture are developed across participating departments;
- A more consistent approach from the different departments can be developed;
- The consistency of information provided by customers to different departments can be tested;
- Trust and understanding can be built across departments.

Joint working arrangements can be set up by having Memoranda of Understanding with other organizations to enable sharing of data and carrying out matching and profiling with their data. This may be facilitated through data warehouses accessible to the organizations involved. The data warehouse can include data from each organization shared through internet, such as the population register which includes data such as driving licenses, passport numbers and electoral rolls. Similarly, data may be shared with external sources also. Joint working may also include co-operation on fraud investigations. This enables departments to identify and investigate cases of common interest, avoiding duplication of effort.

Government departments and agencies should maintain a repository of the cases identified to serve as a ready reckoner along with a list of red flags. Profiling of the fraudsters should also be done and maintained in the repository for reference. The repository should contain detailed description of the case and investigation methodology and sanctions imposed. A detailed profile of the fraudster is an important data maintained in the repository. The information in repository will be a good basis for revising the anti-fraud policy and strategy. Departments should have strict access controls and back-up plans for maintenance of the repository

A.12 Ensure that the efficacy of the anti-fraud mechanism put in place, and continuously monitor and evaluate the fraud-risk strategy

It is important to continuously monitor and assess the performance of the strategies that are formulated to counter fraud. Any leakages that are observed despite the controls should alert the (fraud risk) manager of the need to re-design the strategy. Internal audit provides an independent and objective opinion on risk management, controls and governance by measuring their effectiveness in achieving the organization's objectives. Self-assessment questionnaires can also provide the necessary assurances on the effectiveness of the strategies. Third-party inspections, setting of Compliance Review Teams can also contribute to the overall assurance.

Setting targets and monitoring performance

Departments have to set targets to stabilize or reduce fraud over a period of time. Focusing targets on the overall level of fraud or loss is a good way of assessing performance. Measures of performance include changes in levels of loss, the cost of tackling fraud compared to the return obtained and the rate of recovery of detected frauds.

Performance data on outcome targets may not be available until long after the period measured due to the amount of work involved in sampling cases, checking, calculation and validation of the results. To monitor performance in-year, Departments may rely on output results to indicate whether the outcomes are likely to be achieved. For example, departments may monitor:

- the results of operational checks on transactions;
- fraud investigation activity and outcomes
- number and types of sanctions imposed
- rate of recovery of defrauded amounts detected

Measuring the Effectiveness of the Fraud-risk Strategy

It is essential that assurance about the effectiveness of actions taken to reduce the risk of fraud be obtained. The person assigned responsibility for the management of anti-fraud activities will need to be aware of the many different ways that assurances can be obtained:

a. 'Stewardship Reporting' - This is where designated officers report upwards to the Secretary / CEO at least annually, through the mechanisms established for risk ownership, assurances on the work they have done to manage risk and operate the appropriate control procedures; and

b. Internal Audit. The primary role of internal audit is to provide an independent and objective opinion to the Secretary on risk management, control and governance, by measuring and evaluating their effectiveness in achieving the organisation's agreed objectives. Internal audit also provides an independent and objective consultancy service to help line management improve the organisation's risk management, control and governance.

A.13 Create an independent institution to oversee the implementation of the Policy.

The counter fraud strategy will strive for systemic improvements in the implementation of internal controls in individual departments or units of a Department. There could be an independent body e.g. an anti-fraud unit, which would oversee and administer the counter-fraud practices in the government or department as a whole. The Vigilance Commission and Director General (Vigilance and Enforcement) could be the state level agency to oversee the fraud control activities. Similarly the Chief Vigilance Officers in the departments and Vigilance Officers in agencies under the government could be placed in charge of anti-fraud activities of the concerned department / organization.

Presently, the vigilance bodies are engaged primarily in investigation of frauds as and when they occur. The scope of their work should also include wider responsibilities of preventing and deterring the fraudster. The central unit would also act as a nodal agency enabling joint working of different departments, maintaining data that is vital for the detection of fraud, maintain repository of the cases for future references; support the Departments in detecting and investigating fraud; protect the whistleblower, etc. It should also conduct fraud awareness campaigns for the citizens to help them understand their rights and duties in effective fraud prevention.

Objectives of anti-fraud units shall be:

- Create anti-fraud culture
- Maximize deterrence of fraud
- Successfully prevent fraud which cannot be deterred
- Promptly detect fraud which cannot be prevented
- Professionally inquire into detected fraud
- Obtain imposition of effective sanctions, including appropriate legal action against people committing fraud
- Employ effective methods for seeking recovery of money defrauded

A.14. Disclose information about frauds

Although frauds involve government departments and agencies, the ultimate victims are all of the people of the state. It is important that government departments and agencies are accountable to the public and that the public is fully informed of how they are managing the risk of fraud.

It is recommended that all government departments and agencies adopt a policy and practice of reporting all cases of fraud in their annual reports. At a minimum, information that should be included that allows the reader to determine:

a. How many frauds were detected and how much they cost the community;

b. The nature of the fraud and what operations or units were involved;

c. What was done to prevent a recurrence; and

d. How the perpetrator was dealt with.

The advantages of this would include:

a. Informing the public;

b. Enhancing the accountability of organisations;

c. Raising awareness of fraud and the need to prevent it;

d. Encouraging organisations to prevent fraud and to find cases quickly; and

e. Demonstrating an organization’s commitment to openness and accountability.

In reporting fraud in an annual report or other publication, government departments and agencies should take care to ensure that the information published does not lead to the constructive identification of a person who has not been the subject of a finding. It is also important to ensure that any reports do not prejudice any legal action that might be taken.

Appendix A

SAMPLE ANTI FRAUD POLICY[7]

Introduction

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

Scope of Policy

This policy applies to any irregularity, or suspected irregularity, involving employees as well as vendors, contractors, consultants, outside agencies, and/or any other parties with a business relationship with [department / organisation name). Any investigative activity required will be conducted without regard to the suspected wrongdoer’s length of service, position/title, or relationship to the organization.

Policy

All officers and staff are responsible for the detection and prevention of fraud, misappropriations, and other irregularities. Fraud is defined as the intentional, false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury. It is expected that every officer / employee will be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity.

Any irregularity that is detected or suspected must be reported immediately to the [name / designation of officer], who coordinates all investigations with both internal and external groups.

Actions Constituting Fraud

The terms defalcation, misappropriation, and other fiscal irregularities refer to, but are not limited to:

- Any dishonest or fraudulent act.
- Misappropriation of funds, securities, supplies, or other assets.

[7] The Anti Fraud Policy should be closely aligned to provisions contained in the Financial Rules and other government instructions. This is a generic policy for adoption by any type of organization.

- Impropriety in the handling or reporting of money or financial transactions.
- Disclosing confidential information to outside parties.
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Company. Exception: Gifts less than [Rs ________] in value.
- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment.
- Any similar or related irregularity.

If there is any question as to whether an action constitutes fraud, contact [name / designation of officer] for guidance.

Responsibilities

[General Financial Rules / Financial Code, as applicable] set out the responsibilities of departments in relation to fraud.

The Secretary to Government / Head of Department / CEO 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. [name / designation of officer]. His / her responsibilities include:

i. 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;

ii. Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in the fraud risk profile;

iii. Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;

iv. Establishing appropriate mechanisms for:

   - reporting fraud risk issues; and
   - reporting significant incidents of fraud to the Secretary / HoD / CEO / Accountant General / Police as required;

v. 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;

vi. Developing skill and experience competency frameworks;

vii. Ensuring that appropriate anti-fraud training and development opportunities are available to appropriate staff in order to meet the defined competency levels;

viii. Ensuring that vigorous and prompt investigations are carried out if fraud occurs or is suspected;

ix. Taking appropriate legal and/or disciplinary action against perpetrators of fraud;

x. Taking appropriate disciplinary action against supervisors where supervisory failures have contributed to the commission of fraud;

xi. Taking appropriate disciplinary action against staff who fail to report fraud;

xii. Taking appropriate action to recover assets;

xiii. Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Heads of Offices at district and below level shall be responsible for:

- Ensuring that an adequate system of internal control exists within their areas of responsibility for 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 and 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 Secretary / HoD / CEO 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 staff 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;
- Ensuring that he notifies the government of any conflict of interest;
- 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.

Reporting Procedures

An employee who discovers or suspects fraudulent activity will *contact [name of the designated officer] immediately*. The employee or complainant may remain anonymous[8]. All inquiries concerning the activity under investigation from the suspected individual, or any other inquirer should be directed to the ____________ Unit. No information concerning the status of an investigation will be given out. The proper response to any inquiries is: ‘I am not at liberty to discuss this matter’.

The reporting individual should be informed of the following:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case, facts, suspicions, or allegations with *anyone* unless specifically asked to do so by the ____________ Unit.

Confidentiality

[Organization / department] treats all information received confidentially.

Any employee who suspects dishonest or fraudulent activity will notify the [contact number or name of the officer] immediately, and *should not attempt to personally conduct investigations or interviews/interrogations* related to any suspected fraudulent act.

[8] It is for the Government / Organization to decide, as a matter of policy, whether or not to entertain anonymous complaints.

Investigation results *will not be disclosed or discussed* with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputation of persons suspected but subsequently found innocent of wrongful conduct and to protect the organization from potential civil liability.

Investigation Responsibilities

The [name of investigating agency] has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. If the investigation substantiates that fraudulent activities have occurred, the (name of investigating agency) will issue reports to appropriate designated personnel.

Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

Decisions to prosecute or refer the results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in consultation with legal counsel and ………., as will final decisions on disposition of the case.

Authorization for inquiring into suspected fraud

The Inquiry Officer will have:

- Free and unrestricted access to all records and premises, whether owned or rented.
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

Sanctions

The recommendation of the investigation unit will be reviewed for approval by the designated officers / authorities before any such action is taken.

Administration

[Designation] is responsible for the administration, revision, interpretation, and application of this policy. The policy will be reviewed annually and revised as needed.

APPROVED

Head of Government / Department / Organization

Appendix B

Commonly found Frauds in Major Areas[9]

Cash and cheques

- **Theft of cash (Skimming) –** This involves withholding recording a receipt (a revenue or refund item) in the books for sometime thus retaining with oneself the cash for a temporary period.
- **Theft of Cash (Lapping) –** Lapping is a method of concealing skimming and it could go on for long periods. It involves crediting of one account (which has been 'stolen') with the receipt from another. To illustrate, cash received from tax payer A is not accounted, but is made good with payment received from tax payer B, whose account is made good with payment received from tax payer C and so on.
- **Permanent misappropriation of cash –** cashier or person dealing with cash misappropriates cash and conceals the misappropriation by doctoring the account books.
- **Forgeries of cheques and other cheque frauds –** The particulars on cheques such as payee or amount may be altered; or the signature of the authorized officer may be forged.

Assets

- **Employees take assets for personal use**—an employee misappropriates an organization's assets for his/her personal use without attempting to conceal the theft in the organizations books. Or, an employee sells assets for cash without recording the disposal.
- **Assets are sold at less than fair market value**—assets are sold or disposed of at less than fair market value to someone related to an employee. Or, asset disposal may be recorded at a value less than what was received, and the employee misappropriates the difference.
- **Asset requisitions and other documents are used to move assets to another location to facilitate theft**—an employee overstates the amount of supplies and materials needed for a project and takes the excess.
- **Purchasing and receiving functions are manipulated**—an employee receiving goods on behalf of the organization falsifies incoming shipments and takes part of the shipment.

[9] This is based on Asian Organization of Supreme Audit Institutions (ASOSAI) Training material. This is by no means an exhaustive list of frauds.

- **Large unexplained inventory shortage**, particularly of inventory that has resale value. This is a symptom of employee theft of assets.
- **Pilferage of stores, stationery and other assets –** the most common risk in offices and government offices particularly is that of loss on account of theft of stores and other assets by unscrupulous employees.
- **Misuse of assets –** This could involve use of assets for unauthorised purposes such as use of official vehicles and other resources for unauthorised use or for unofficial consideration.

Payroll, expense and credit cards

- **Ghost employees**—a fictitious employee is put on a department's payroll, and payments for that employee are deposited into the perpetrator's bank account or the account of one of his/her family members. With electronic payroll deposits, it is more difficult to uncover ghost employees.
- **Terminated / retired / transferred / repatriated employees are not deleted from the payroll system**—Payments continue to be made to terminated, retired, transferred, repatriated employees, or those who have resigned, or those who are on medical leave. Payroll payments are deposited into the perpetrator's bank account or the account of one of his/her family members.
- **Personal expenses are submitted as business expenditures.** An employee submits personal expenses such as computer accessories, automobile fuel purchases, or personal meals as business expenses.
- **Expenses are submitted twice.** An employee is reimbursed more than once for the same expenses or items that have been purchased and paid for by the entity, and also claimed in an expense report or claim.
- **A claim for expenses that someone else paid for is submitted for reimbursement.** For example, three government employees share a taxi and all three submit the taxi fare on their expense reports. Or, a meal already paid for under hospitality expense or conference is subsequently claimed by an employee as part of his/her daily meal allowance.
- **A false claim for automobile kilometer charges is submitted.** An employee submits a claim for automobile kilometres that is higher than the actual kilometres driven.
- **False LTC, TA and medical claims –** This is again a very common fraud in organizations, particularly government organizations where employees may make false claims of LTC, TA and medical expenses.

For credit cards the following are the commonly found frauds,

- **Personal purchases**—a government employee cardholder purchases goods or services for personal use on their government credit card, without authority to do so, and allows the department or agency to pay for these goods or services without reimbursing the employer. This fraud can go undetected if the goods and services appear to be normal government purchases such as computers, automobile fuel, and travel and hospitality expenses.

- **Unauthorized billings**—an individual who, intentionally and without the cardholder's knowledge, permits the billing of personal or nongovernment items on a government credit card and does not reimburse the government for these purchases. This fraud is often undetected if the government cardholder does not verify all charges on the credit card statement before authorizing the payment of the outstanding balance.
- **Unauthorized charges by retailers, wholesalers, and contractors**—in this kind of fraud, businesses will process charges against government credit cards for goods and services that were never authorized or never provided. This kind of fraud also includes inflating charges on government credit cards that do not reflect the agreed upon amount for the goods and services provided. This fraud goes undetected if the government cardholder does not verify all charges on the government credit card statement against invoices or purchase orders and permits the outstanding credit card balance to be paid.

Contracts (Procurement, Service and Construction)

The following are common methods of perpetrating contract fraud,

- **Bribery and kickbacks—**a contractor gives an employee money, gifts, or other favors in order to obtain business or favorable treatment.
- **Change order abuse—**changes are made to the original contract conditions, resulting in a need for more funds than were provided in the original contract. Change orders may be issued throughout the life of the contract to compensate a contractor who initially submitted a low bid.
- **Collusive bidding, price fixing, or bid-rigging—**a group of prospective contractors may make an arrangement to eliminate or limit competition
- **Co-mingling of contracts—**a contractor bills for the same work under more than one contract.
- **Conflict of interest—**contracts are awarded to organizations that employ government employees or their families, or to companies in which government employees or their families have an undisclosed financial interest.
- **Defective pricing**—a contractor submits inflated invoices that do not comply with the costs/prices specified in the contract.

- **Duplicate invoices—**a contractor submits separately two copies of the same invoice and is subsequently paid twice.
- **False invoices—**a contractor submits invoices for goods that have not been delivered, or the invoice does not reflect the contract terms.
- **False quality and performance representations**—a contractor makes false representations about the quality of the products to be supplied or qualifications to perform the requested services.
- **Information disclosure—**a government employee releases unauthorized information to a contractor to assist that contractor to win the contract.
- **Local purchase order abuse or split purchases**—the total cost of purchasing goods and services exceeds the local authority limit, or a competitive process is required to provide such goods or services. To bypass these rules, the purchases are split into two or more segments.
- **Phantom contractor**— a contractor submits an invoice from a nonexistent company to support fictitious costs contained in a government cost-plus contract.
- **Product substitution**—a contractor fails to deliver the goods or services as specified in the contract. The contractor may substitute an inferior product without informing the government.
- **Progress payment abuse: front-end loading or advance payment**—under government contracts, payments are made as work progresses. The payments are based on the costs incurred, the percentage of work completed, or the completion of particular stages of work. Progress payment fraud normally includes falsified certification of the work completed in order to receive payments prior to the work being done. The contractor may inflate the costs of the initial work so that, when the percentage of completion billing method is applied; the contractor would receive higher cash flows relative to the actual work completed. The cost of subsequent contract work would be understated with the anticipation that change orders would be approved for additional compensation.
- **Purchases for personal use** — a government official purchases items for personal use, or makes excess purchases of which some items are diverted for personal use.
- **Short bidding time limits—**the lead-time for responding to a proposal is unusually short so that only bidders with inside knowledge will be able to prepare a proposal on time. There is no compelling reason to justify a markedly reduced response time.
- **Tailored specifications—**a government official establishes unnecessary or highly restrictive product specifications that only one contractor can meet.

- **Unnecessary purchases—**goods or services that have been previously purchased are purchased again when there is no additional need.

Revenue collection

The following are the frauds commonly found in the area of revenue collection

- **Theft of revenue receivable**—an employee steals revenue received. Or an employee enters only part of the revenue received in the accounting records and pockets the difference. To avoid being detected, the employee posts B's payment to A's account, C's payment to B's account, etc. This process, called **lapping**, requires continuous manipulation and monitoring of many accounts and transactions.
- **Revenue receivable write-offs**—an employee writes off as uncollectible, revenue receivable that are not really in arrears or will likely be collected. This is done to conceal the theft of accounts receivable payments or the future theft of payments.
- **Bribery or kickbacks**—an individual gives a government employee money or gifts in order to receive preferential treatment. For example, an individual gives money to a government employee to obtain surplus Government assets at a low price.
- **Conflict of interest**—a government employee has an undisclosed personal interest that may affect, or be perceived to affect, his/her independence and objectivity in carrying out his/her job responsibilities. In the context of revenues, a government official sells goods or services to a company that employs his/her spouse at lower prices or collects less revenue from an industry on favourable terms than those that could have been negotiated with another company.
- **Disposal of assets for personal gain**—a government employee with a personal interest in government assets could identify those assets as surplus goods even though they still have a government purpose. The sole reason the employee identifies those assets as surplus is to purchase them for personal benefit.
- **Information theft**—a government employee releases information to a third party without charge when the information should have been sold.

Program management

- **Conflict of interest—**having undeclared private interests that could affect, or be perceived to affect, the independence and objectivity of an individual in carrying out official duties. For example, a government official recommends that a program be funded by the government where his relatives are in the management

- **Embezzlement—**taking money that has been lawfully received and using it, without the knowledge and consent of the provider of the funds, for other purposes.
- **False representation**—knowingly making false or misleading statements to gain an improper advantage. In the context of program management, this could involve making false statements to mislead the government in order to obtain funding.
- **Fraudulent concealment**—knowingly hiding information that is necessary and important to the funding decision and program monitoring.
- **Improper or unusual approval authorities**—those approving funding applications do not have the required delegated authority. Or senior officials, who would not normally be involved in the approval process, take a special interest in the approval of the funding application of a program and its subsequent management.
- **Questionable or fraudulent performance reporting—**a funding recipient does not submit all the performance information required by the agreement Or the quality and completeness of the performance is so poor that there are suspicions about how funds were used. Minimum or no performance information may indicate that government funds were diverted to other unauthorized projects or used for personal benefit.

I.T environment

The frauds committed in IT environment are,

- **Altering or falsifying computer input** transactions to conceal problems such as misappropriation of funds or assets;
- **Implementing computer program changes for personal gain** e.g. an employee manipulating systems to have payments made to himself/ herself
- **Stealing computer data** and selling it to third parties;
- **Direct computer file changes** by an employee for his/her benefit;
- **Transferring funds electronically** and subsequently destroying the audit trail; and inappropriately accessing computer information that can be used to commit an illegal activity (e.g. a person hacks into a government computer server and views confidential information that will be publicly announced shortly which will impact on share values of certain publicly traded companies and uses this confidential information to make gains on the stock market.

Computerized fraud and corruption can be categorized according to three stages in processing transactions:

- **Input frauds**. Phony transactions are altered or added to the stream of data being processed. For example, input documents such as invoices are altered, forged and falsified
- **Throughput fraud**. These are the types of computer frauds that tend to be reported in the press. A computerized "wizard" alters the programming to achieve some desired result. For example, a program that calculates interest earned on savings accounts at a bank is changed so that rounded amounts (fractions of pennies) are deposited into an account controlled by the computer programmer.
- **Output frauds**. Output reports, documents or files are altered, suppressed or stolen. For example, exception report used for internal control purposes may be altered to conceal a defalcation.

Commonly found internet fraud include**,**

- **Theft of funds through false Government Online applications**;
- **Identity theft** or using such stolen identity through the Internet;
- **Illegal use of government credit card numbers** for purchases on the Internet;
- **Stealing data via the Internet** for personal benefit or selling it to third parties;
- **Sabotaging computer systems**, including planting viruses and worms by hacking into computer systems via the Internet, which affects network downtime and destroys valuable computer information;
- **Sending endless SPAM** to government Web sites

B: Preventing Fraud

Despite best measures to deter fraud, there will still be attempts to commit fraud. If deterrence is the first line of defence, prevention is the second line of defence in fraud control. Government / organization should develop the most effective preventive measures duly incorporating the lessons learned. A holistic approach combining system / process redesigning and implementation of control measures will successfully prevent most attempts of fraud.

An important evidence of sound system of prevention measures is the continued movement towards sharing good practice through guidance, highlighting lessons learned and by the analysis of frauds that have been attempted or that have occurred and their publication in an annual report by the department.

Given below are some questions that the department / organization might like to itself to check if the preventive practices are adequate. A more detailed score card to assess effectiveness of preventive controls is given in Appendix C at the end of this section.

Check List of questions

Whether your organisation:

- ensures fraud controls are applied consistently and their effective functioning is monitored by the management and through Internal Audit?
- considers strengthening controls where new fraud risks appear or where fraud starts to escalate?
- considers fraud proofing of new programmes?

B.1. *Prevent fraud through effective internal controls*

The concept of internal control has evolved in the context of corporate failures and over a period of time. Finally, a framework of internal controls developed under the aegis of COSO (Committee of Sponsoring Organizations) has come to be accepted world over as the benchmark. This framework has been further enlarged to an Enterprise Risk Management (ERM) framework. A short note on the COSO Internal Control Framework is given at the end of this section in Appendix D.

There are a range of controls viz. physical checks, reconciliation, supervisory checks, segregation of incompatible duties, etc. that address risks, including fraud. The consistent application of internal controls can be highly effective in preventing frauds. Controls need to be designed which are proportionate to the risk, while enabling the organization to deliver the services to its customers to meet their needs.

Ensure audit trails

All work practices, project plans and procedures should have auditable features included in their design. Staff should be encouraged to recognise the value of ensuring that the nature and reasons for all their decisions are recorded and accessible for audit. This is particularly so for those involving fraud risks.

Balance Fraud Controls and Service Delivery

Internal controls meant to minimize chances of fraud taking place should not unnecessarily hinder the agency’s ability to deliver services. For example, welfare benefits or health care must be provided in a timely fashion and without undue harassment of beneficiaries. The nature and intrusiveness of controls in place to prevent fraud must be weighed against the level of customer service. To do this, the controls should be tested to ensure that they will prevent fraud but without adversely affecting the service delivery. Testing controls may indicate that not all of them are necessary or that they can be done differently to reduce any delays in processing. Reviews of controls should be undertaken on a regular basis to make sure they remain useful. For example, it may happen that the employees have developed a work-around that makes their job easier but makes fraud easier to commit.

A survey or focus group may be used to test public attitude including the staff attitude to the controls and their compliance with controls to prevent fraud. The findings from such research can help identify opportunities to improve prevention and to strengthen internal controls, identify any messages that need to be reinforced, reveal any areas where compliance with prevention controls is insufficient.

Identify and deal with high risk positions

Most organisations have positions that present the opportunity to participate in fraud. These represent high risk positions. These are positions with a high degree of discretion and those making decisions that have high cost or reward impacts. It should be ensured that occupants of the positions are:

a. Frequently rotated between duties, territories, etc.

b. Regularly involved in individual discussion with supervisors about their duties and relationships;

c. Properly supervised; and

d. Monitored to ensure they follow procedures.

Besides high risk positions there might be geographic hotspots (some locations having more than normal share of frauds or remote locations that are more prone to frauds) and blacklist of vendors, contractors, etc. that need a special watch.

Ensure physical security

While fraud always involves a degree of deception, it can also involve a physical dimension:

- Cash might be carried away by some means;
- Data might be accessed directly in the workplace, bypassing access controls such as firewalls;
- Records might be accessed or copied outside work hours or by unauthorised persons; and
- Documents containing confidential information may simply be left lying around and be discovered by opportunists.

There are also a number of organised groups and individuals who simply move around office buildings looking for opportunities. They look for poorly secured information such as accounts, credit cards or credit card receipts, or order form numbers. They can use this information to perpetrate frauds against the organisation or members of staff. Documents such as stored cards, cheques or order forms can be stolen and fraudulently negotiated.

Government offices / organisations need a system to deny unauthorised people access to their premises and to monitor and record who does enter them. Access denial involves active access control. Access to resources needs to be controlled so that they can be used legitimately. Access controls should give authority to enter premises and to enter any part of premises. The system records such movements. This helps to detect, as well as to deter, unauthorised access to premises.

Each activity presents its own risk and requires an internal control that addresses that risk. For example, a payment to a beneficiary under a health programme would be specific to the nature of benefit and the manner of its disbursement. While this is so, there are a large number of areas that are common to most departments, agencies and activities where applicable controls would also be common. Every department should design controls that address specific risks that its activities and programs face as required by good practice A.6. above. Given below are some internal control measures that are applicable to areas common to most departments such as payroll, asset management and so on.

Fraud Area / risks	Mandatory Controls
Cash	• 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 should be kept to a minimum, recorded and checked periodically.
Unauthorized bank accounts and Multiple bank accounts	Government money is expected to be kept in government account. However, these days there is a widespread practice of opening multiple accounts, which poses a major risk of fraud. • The government / organization should have a clear policy regarding opening of bank accounts. The policy should provide for the exceptional circumstances for opening a bank account outside the government account and carry necessary checks and balances.
Unauthorised use of cheques and payable orders	• Financial stationery (blank cheque leaves) 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

Fraud Area / risks	**Mandatory Controls**
	are sent are correct. For large value payments check encashment to ensure that the intended recipient acknowledges 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 Rs. 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.
Theft or unauthorised use of assets Risks in this area include use of assets for personal gain or misappropriation of assets	• Asset register to be maintained up to date. • 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.
Income / Revenue	• Always issue pre-numbered receipts. • Maintain accurate records of income received. • Duties related to opening letters (dak) 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: ▪ Letter 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;

Fraud Area / risks	Mandatory Controls
	•
Income / Revenue Theft of income and funds disguised by manipulation of accounting records	• Always issue pre-numbered receipts. • Maintain accurate records of income received. • Duties related to opening letters (dak) 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: ▪ Letter 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; • Formal procedures of delegation should exist for authorising total or partial write-off of a debt, • Regular supervision and test checking of work should be carried out by staff involved in the accounting for income and the handling of cash. • Regular reviews should be conducted of all income generating activities and results compared with an estimate of expected income / revenue. • Arrears greater than a set amount or over a certain age should be regularly reported to senior management. • There should be a standard system for recording and billing all goods and services. • Reductions in debtor amounts should be accompanied by an authorised credit note. • Rotation of staff.
Misallocating income to pay off debts of associates	• Bank pay-in slips should be checked regularly on a random basis to detect teeming and lading. [**Teeming & lading** is another common method of misappropriating the customer cash payments. This involves holding back all or part of a day's collections and banking them at a later date. For example, a receipt is not issued in respect of a payment by a cheque,

Fraud Area / risks	Mandatory Controls
	which is then banked to cover cash collections (which have been receipted) to the same or similar value. The payee may not demand a receipt under the impression that the cheque leaves a trail and so a separate receipt may not be needed.] • Records of receipts should be reconciled with amounts deposited in the bank and discrepancies followed up independently and promptly. • Each bank deposit should be supported by a list of cheques referenced back to the debts to which they relate. • Staff involved in accounting for income should be independent of those collecting income. • Duties are segregated to ensure that account statements should be sent to debtors separately of sales, income and cash accounting staff. • The accounts receivables balances should be updated for receipts within 24 hours.
Fake invoices created by employees.	• Systems should exist to ensure that purchasing department staff is able to make payments to suppliers and access to a certain supplier is not restricted to a single manager or employee. • Checks should be made on invoices in all instances to ensure that they correspond to the supplier detail stored on the computer system.
Human Resources Fraud **Payroll Fraud**	• Regular checks of the payroll master file should be carried out by the Personnel Department to ensure that the basic salary and allowances are correct. • Regular computerised ‘reasonableness checks’ should be performed to highlight issues such as particularly high claims for overtime. • All overtime approvals should be evidenced. • Timesheets which include overtime should be subject to the same controls as normal payments. • Urgent or emergency payments should be subject to the same controls as normal payments. • Departmental officers should receive and check standing payroll on a regular systematic basis. • Ensure that, wherever possible, all payroll changes are made by a personnel function that is organisationally separate from payroll function.

Fraud Area / risks	Mandatory Controls
	Only Personnel Section 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 Section who should independently confirm the existence of new recruits and that rates of pay to be paid to starters are correct. • Produce listings of all new recruits, those who have left the organization 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 for investigation by management. • Subject the payroll master file to periodic checks by personnel to ensure that each post is authorised, that the correct person is in post, that the person exists and that basic salaries and allowances are correct.
Ghost employees	• Procedures should exist to ensure that returned cheques, unpresented cheques and unclaimed cash wages are followed up. • Personnel and payroll functions should be separated. • Approval of salaries following general pay reviews should take place. • Staff should be made aware of internal policies and procedures in respect of payroll. • Payroll staff should be required to take their annual leave entitlement. • Work undertaken by payroll staff should be reviewed and test checked by supervisory officers on a regular and spot basis. • Access to human resources and payroll data should be restricted. • The Payroll Department should be promptly notified of staff leaving and newly joining. • Amendments to payroll master file, including new

Fraud Area / risks	Mandatory Controls
	recruits / those joining on transfer, those leaving on transfer, superannuation, resignation, etc. and changes in pay levels and bank account details, should be independently checked and authorised. • Dispatch and distribution of cheques should be carried out independent of the payroll section.
Travel and subsistence fraud.	• Expense claims should be checked against receipts and checked for eligibility, reasonableness and consistency. • Expense claims should be independently authorised by a designated manager or Director. • Reimbursements should not be processed without receipts. • Claims should not be submitted by one employee on behalf of another. • Ensure that countersigning officers pass approved claim forms direct to the finance team. • Instruct countersigning officers to initial amendments to details on claim forms and finance teams to reject any claims where amendments have not been initialed. • 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 countersignatories. • 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.
Contract fraud A contractor could be selected as a result of favouritism or who does not offer best value for money. Payments made for work not carried result of collusion between the contractor and official.	• Documented policies should be in place requiring approval for the receipt of gifts and hospitality, declaration of any interest and outlining who can commit the organisation to expenditure. • Standard invitation to tender documents should exist. • It should be ensured that contract specification is not written in a manner that it favours a particular supplier. Contracts should contain precise

Fraud Area / risks	Mandatory Controls
	specification of the work, goods or services to be provided. A panel of technical, end user and financial representatives should be involved in drawing up the specifications. • It should not be possible for contract conditions to be changed to accommodate a favoured supplier, or to exclude competitors. For this standard contract conditions and specifications should be used. Any variations should be approved by senior management. • 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 committee against the agreed evaluation criteria. • Staff should be required to declare any personal interests they may have which may affect the tendering process. • Original evaluation criteria should not be changed after the receipt of tenders. The evaluation criteria should be furnished to suppliers. • Variations of a contract should be authorised by an appropriately qualified person. • All results of tendering exercises, above an agreed level should be reported to the top management. • The ultimate supplier selection decision should be properly documented and a file maintained which includes details of all competing tenders. • Ceilings should be set for total variances in contracts which require further senior management approval. • Formal contracts, signed by both parties, should exist and be held in a secure location. • Certification of contract delivery should be independent of officers involved in awarding the contract. There should be clear separation of duties between ordering the work, certification and authorization of payment. • Contractors with poor performance record should be black listed / removed from approved suppliers

Fraud Area / risks	Mandatory Controls
	list. • 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. • It is advisable that the department / organization formally request the tenderer to sign a document confirming that no fraud or corrupt practice has occurred at bid submission stage. This has two benefits: √ It acts as a deterrent – tenderer is alerted to the fact that the client is aware of the risk of fraud and will be on the lookout for any evidence that it has occurred. √ It ensures that should something fraudulent come to light, tenderer can have no excuse that they were unaware of the client’s policy.

Fraud Area / risks	Mandatory Controls
Risks associated with grant funding. 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. • An officer with the appropriate delegated authority should give the final approval for a claim. • 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 been paid out and that they have gone to the correct recipients. • Systems operated by organisations who receive grant funding for specific projects should be reviewed to ensure that the spending of grant monies is adequately controlled.

Fraud Area / risks	Mandatory Controls
Cards/ credit cards.	• All purchases should be approved by the budget holder who should not also be a card-holder. • Use suppliers with whom the department has a contractual relationship or is otherwise a reputable merchant. • Departments should appoint an individual to be the cardholder manager who will be responsible for appointing cardholders and for dealing with the card-issuing bank. • The card-issuing bank should distribute the cards to a point in the department agreed with the departmental cardholder manager. The cardholder should sign the card in the presence of the card holder manager. The department should maintain an up to date list of all its cardholders. • Cards should only be issued by the bank upon request by the card holder manager. • Cards must be returned to the cardholder manager when cardholders move or cease to be cardholders. The cardholder manager should ensure that the card is destroyed and the record of cardholders amended. • Departmental policy and advice on using GPCs should be clearly documented, kept up to date and effectively communicated to all staff. • Cardholders must hold cards securely. • Cardholders must check all entries on statements supplied by the bank and refer any discrepancies to the cardholder manager. • Budget holders should carry out periodic checks to ensure that GPC statements are properly reconciled and that only authorised purchases are made.

Fraud Area / risks	Mandatory Controls
Orders placed on the Internet fail delivered or goods received are not of the desired quality	• Make sure your browser is set to the highest level of security notification and monitoring. • Check that you are using the most up to date version of your browser and ensure their security features are activated. • Keep a record of the retailer's contact details, including a street address and non-mobile telephone number. Beware if these details are not available on the website. Do not rely on the e-mail address alone. • Click on the security icon to see if the retailer has an encryption certificate. This should explain the type and extent of security and encryption it uses. Only use companies that have an encryption certificate and use secure transaction technology. • If you have any queries or concerns, telephone the company before giving them your card details to reassure yourself that the company is legitimate. • Print out your order and consider keeping copies of the retailer's terms and conditions and returns policy. Be aware that there may well be additional charges such as postage and VAT, particularly if you are purchasing goods from traders abroad. When buying from overseas always err on the side of caution and remember that it may be difficult to seek redress if problems arise. • Check statements from your bank or card issuer carefully as soon as you receive them. Raise any discrepancies with the retailer concerned in the first instance. If you find any transaction on your 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 card details, find another method of payment.

Fraud Area / risks	**Mandatory Controls**
Theft of sensitive/restricted documentation or information.	• All data should be stored securely and adequately backed up. • Personal data should be held in accordance with the required statutory provisions (e.g. fairly and lawfully processed; processed for specified purposes; not excessive; accurate; not held for longer than necessary; processed in line with data subject's rights; secure; not excessive, not transferred to countries where the rights of data subjects cannot be adequately protected). • Procedures should be in place to provide data subjects with access to data held about them if required under law. • Access to computer records should be logged and spot checks made to confirm that there were valid reasons for any unusual accesses. • Computer logs should be adequately protected against unauthorised access and amendment
Information Technology Applications	• Computer systems are developed and maintained in an authorized and efficient manner to establish control over changes to application systems, testing, conversion, implementation and documentation of new or revised systems and access to systems documentation. • Computer systems are used only for authorized purposes and only by authorized personnel. • Errors are detected before, during and after processing. • Systems software modifications are appropriately authorized, approved, tested, implemented and documented and that access to software and documentation is restricted to authorized personnel. and • Transactions being entered into computer systems are appropriately authorized and access to data and programs is restricted to authorized personnel.

Fraud Area / risks	**Mandatory Controls**
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 defined process. Suspense accounts should be reviewed on a regular basis to confirm their validity.

B.2. Re-engineer processes to prevent (reduce the risk of) fraud

Complexity of process / schemes can result in higher risk of fraud. An effective way of preventing frauds and errors would be to review and simplify the processes and schemes. Many a time, a complex process provides an opportunity for fraud as it cannot be either adequately controlled or it is too expensive to control.

To illustrate, after the stamp paper scam, Government of Andhra Pradesh has decided vide GO Ms. No. 953 dated 10.9.2003 to restrict the use of non-judicial stamp paper up to value of Rs 100 denomination; payment of remaining stamp duty is now made through payment in the designated branches of State Bank of Hyderabad. Similarly, the dematerialization of securities (share and debenture certificates) where the certificates in physical form were replaced by digitized records held by National Securities Depositories Limited has helped reduce the fraud risks such as counterfeit certificates, theft of certificates, etc.

B.3. Assess the inherent risks of the new schemes/ programmes and fraud proof the schemes/programmes

The Departments have to fraud proof new programs and systems since there are greater chances of occurrence of fraud whenever new schemes or programmes are introduced. Organizations need to recognize their responsibility when designing and implementing new policies, programmes and systems to build in good controls to manage fraud where there are vulnerabilities, or to fraud proof them by designing them to be inherently less vulnerable to fraud. Sufficient weight should be given to expert advice on the risks of fraud in new programmes and effective counter fraud measures should be integrated into the design.

Where innovative schemes are being proposed, it is good practice to pilot these to identify any further risks of fraud. Early consultation with internal audit and counter fraud specialists can help to identify the risks, and to obtain advice on how these can be minimized, at key stages during design and implementation of new programmes. An evaluation process is helpful in determining whether early risk assessments have been effective in countering fraud risks during development, piloting and initial implementation.

B.4. Prevent information/data fraud

Many frauds involve obtaining information by deception and then using that information to obtain more tangible benefits. With the development of the information economy, data is taking on a value equivalent to cash. It can also be converted to, or used to obtain, cash.

Insiders perpetrate most data frauds. Organisations are also at risk of fraud via remote telecommunications access. Protecting electronically stored data is a challenge of the times. The data must be protected against unauthorised access from within and also from outside. To guard data holdings, organisations should:

- Make clear risk-based decisions about who has access to what data, and to what level. Banking and payroll systems are especially sensitive and need to be protected from improper access.
- Issue everyone who accesses data with unique login identification. In conjunction with a password, this should be required for all accesses
- Enforce the use of logins and passwords so you can tell when data is accessed, updated, amended or deleted and by whom. Logins and passwords must not be used by more than one staff member and should never be shared
- Encourage the use of passwords that contain both alpha and numeric characters. These offer many more combinations than those only containing digits or letters and are much more difficult to break. They should be used wherever practicable
- Record and monitor all access to data. Records should also be available for audit
- Ensure that staff log off from or lock unattended computers
- Make it clear using another officer's password will not be tolerated. This should be dealt with in the organisation's disciplinary arrangements, training and induction
- Passwords should be regularly changed. They should also be changed when a person thinks someone else might have found out their password
- Organisations that provide electronic access for branch offices, field staff, customers and the community should install firewalls to protect against unauthorised access

B.5. Prevent fraud in relation to identity

Identity fraud may be defined as an individual falsely representing him or herself as either another person or a fictitious person to an agency for some benefit. This misrepresentation is supported by fraudulently obtaining or falsely reproducing documents.

Identity fraud is a major problem and a growing one. People who succeed in impersonating another individual often obtain information, services and goods fraudulently. Because they can quickly disappear with the proceeds, perpetrators are unlikely to be caught.

Using freely available modern technology, it is now possible to forge many documents commonly used for identification purposes. Fraudsters can readily produce driver's licences, passports and birth certificates. The forgeries are often all but undetectable to the untrained eye. This means that the traditional ways of identifying people are not now sufficient. Alternative means of identification are being developed as the threat of forged documents becomes greater.

Despite this, documents will still be important to the identification process for some time to come. This is because presently available alternatives for identifying individuals are comparatively too slow, cumbersome, expensive and unreliable.

As with other types of fraud, agencies need to put into place prevention and detection strategies to control possible identity fraud. Identifying the person registering for benefits or services is a vital first step for agencies to ensure they maintain their own and the public's confidence in the integrity of their operations. Without such confidence, agencies will be unsure of the citizen's entitlements to benefits and services, and leave themselves vulnerable to fraud.

Some of the counter measures to prevent identity fraud are:

- identifying documents of higher integrity to be the only documents accepted by departments as proof of identification;
- having a more rigorous procedure for dealing with applicants who supply no identity documents;
- using key identity data as proof of identity and storing it on agency databases for checking;
- using powerful online computerised searching facilities to ensure no previous records exist for new applicants;
- having a common database containing the details of lost or stolen document details and false identities;

- removing multiple registrations of the same customer from databases; and
- developing an online gateway for mutual use in confirming State and local government documents such as drivers licences and birth certificates.

Organisations need to develop methods and procedures that allow them to verify that documents are genuine. The best way to do this is to firstly identify the circumstances where the risks of adverse consequences due to relying on unauthenticated documentation are high. Where the risks are high, the departments should contact the issuing organisation and ask for some form of verification. Sometimes it may be necessary to delay finalising a transaction while these checks are done. If an organisation regularly relies on documents provided by a particular agency, it should be able to develop a procedure for quickly verifying documents.

Identity fraud has to be seen from two sides –

a. how a government organization would protect itself from disbursing benefits to persons with (fraudulently obtained) false identities; and

b. equally importantly, how a government organization responsible for creating identity information and documents protects such information and documents (e.g. birth certificates, passports, electoral card, driving license, ration card, etc.) from being fraudulently copied, stolen etc.

It is important to remember that ‘if a public sector agency accepts a false document as proof of an applicant’s identity, the applicant can obtain a genuine document from that agency, either in their own or a false name, to which they are not entitled. This genuine document can then be used to obtain other genuine ID documents or services in that name.’

Protecting identity information and documents

In so far as protecting identity information and documents is concerned, the risks can be categorized under the following seven heads:

a) Physical security
b) Information security
c) Document security features
d) Authentication
e) Staff
f) Outsourcing

Physical Security

Physical security refers to the arrangements an agency has in place to protect its premises, information, equipment, and materials used in the production of ID documents from theft, damage or misuse by staff or outsiders. This includes secure handling, storage and transportation. In relation to ID documents, materials could include security paper, blank printed forms, watermarks, holograms, etc. An agency with inadequate or inappropriate physical security arrangements for its needs could be at a higher risk of misuse of ID information and related equipment and materials by staff or outsiders.

Information security

Information security relates to the secure handling, storage, access to and transmission of all types of ID information or ID documents held by an agency, both in hard copy and on computer. Government agencies are repositories for significant amounts of ID information about members of the public, such as names, dates of birth, addresses and financial information. This type of information is an extremely valuable commodity with particular usefulness for individuals wishing to fraudulently create or assume identities, or contact a person for improper or illegal purposes.

Document Security features

Technological advances have made forging documents much easier. Desktop publishing equipment continues to decrease in cost and improve in quality and availability. Agencies need to be aware of higher-order security features such as watermarks. It should also be recognized that photographs do not necessarily provide sufficient protection against forgery. Nor can agency staff often be completely confident that the ID documents that seemingly possess the correct security features are authentic documents, legitimately belonging to the person presenting them.

It would be impractical to suggest that all ID documents should contain the level of security features of a passport or even a driver's licence. However, agencies should consider this issue and make informed decisions about what security features are required to ensure the level of protection warranted for each type of ID document produced. As part of their ongoing review practices it would be worthwhile for these agencies to revisit the issue on a regular basis to ensure they are making the best use of the available technology.

ID documents include some sort of identifying feature, such as individually numbered or bar-coded paper or forms, which can be used as a means of authentication if another agency wishes to check the authenticity of an ID document that has been presented to it.

Authentication

'Authentication' refers to the process of determining that the ID documents presented with an application were issued in their present form by the nominated agency and legitimately belong to and accurately identify the person making the application. Authentication involves answering two main questions:

- Are the applicants who they say they are?
- Are the documents they present genuine and legitimately theirs?

Staff

An agency's staff has access to the agency's systems and data holdings of ID information and has a role in creating ID documents. Agencies should be fully aware of the risk of staff misusing their positions and their computer access or taking advantage of poor data control systems to obtain a benefit for themselves or others.

Outsourcing

Some agencies may outsource some part of the process related to the creation or issue of an ID document or the storage of ID information. However, agencies should be aware that, although outsourced, the function and the risks associated with it remain the agency's responsibility. Functions which may be outsourced include:

- computer services,
- manufacture, transport or storage of equipment or security materials such as paper, holograms, etc,
- digital or hard-copy data and record storage, or
- some part of the assessment procedure.

Agencies should also be very aware that consultants and contractors not involved in functions related to identity information or documents can take advantage of inadequate computer or other controls to access and misuse or steal information, equipment or materials.

Outsourcing a function removes it from the direct control of the agency and may subject it to different standards. Without proper risk treatment strategies in place, outsourcing can expose an agency to greater corruption risks than undertaking that function itself. For example, off-site contract staff is not subject to agency supervision and discipline or performance management and may not have received the same level of training. They may not have been well screened prior to employment. Even contract staff, who perform their duties on agency premises may not have been as well screened or trained prior to their employment as agency staff. In addition, the environment at the contract site, including computer and physical security, may not be up to the agency's standard.

Preventing forgeries of cheques

A related authorization strategy which has been highly successful in preventing cheque fraud is the positive pay system provided by various banks. Businesses are able to provide their banks with electronic lists of cheques issued each day, which are immediately reconciled with cheques actually presented. Any forged or altered cheque will then be detected and payment stopped. Not surprisingly, this practice is in-built in treasury bank advice system where a list of cheques issued is separately sent to bank.

Preventing counterfeiting

Another means of reducing the risk of counterfeiting is to impose controls on the availability of raw materials used in the manufacture of (counterfeit) cards, documents and currency. The companies producing raw materials or machines should educate the staff about security and to monitor unusual requests for materials which could be used for counterfeiting.

B.6. Prevent staff (insider) fraud by proper vetting and security screening of employees and third parties

An important part of an effective fraud and misconduct prevention strategy is the use of due diligence in the hiring, retention, and promotion of employees, agents, vendors, and other third parties. Such due diligence may be especially important for those employees identified as having authority over the financial process.

The scope and depth of the due diligence process typically varies based on the organization's identified risks, the individual's job function and/or level of authority, and so on.

'The lack of employee recruitment checks and controls in some organisations lies at the heart of the employee fraud problem. They are the first line of defence in stopping the criminals placing individuals inside your organisation.' CIFAS research, *Employee Fraud: The Enemy Within*

Tackling Staff Fraud and Dishonesty: Managing and Mitigating Risks – A Chartered Institute of Personnel and Development (CIPD) and CIFAS, U.K. Guide provides many useful insights into staff fraud and how to tackle them.

Appendix C

Fraud Prevention Scorecard
(to assess effectiveness of preventive measures)

To assess the strength of your organization s fraud-prevention system, carefully assess each area below and score the area, factor, or consideration as either:

🔴 indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level.

🟡 indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level.

🟢 indicating that the area, factor, or consideration is strong and fraud risk has been reduced at least to a minimally acceptable level.

Each area, factor, or consideration scored either red or yellow should have a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud-prevention Area, Factor, or Consideration	***Score***	***Notes***
Our departmental culture and tone at the top is as strong as it can possibly be and establishes a zero-tolerance environment with respect to fraud.		
Our department’s top management consistently displays the appropriate attitude regarding fraud prevention and encourages free and open communication regarding ethical behavior.		
Our Code of Conduct has specific provisions that address and prohibit inappropriate relationships whereby officers or employees could use their positions for personal gain or other inappropriate purposes.		
We have adequately assessed fraud risk for our organization based on known frauds that have occurred in similar organizations, in-house fraud brainstorming, and periodic reassessments of risk.		
We have adequately addressed the strengths and weaknesses of our internal control environment and have taken specific steps to strengthen the internal control structure to help prevent the occurrences of fraud.		

Fraud-prevention Area, Factor, or Consideration	***Score***	***Notes***
We have a strong internal audit department (if applicable) that functions independently of management. The charter of our internal audit department expressly states that the internal audit team will help prevent and detect fraud and misconduct.		
We have designated an individual with the authority and responsibility for overseeing and maintaining our fraud-prevention programs, and have given this individual the resources needed to manage our fraud prevention programs effectively.		
Our human resources department conducts background investigations with the specific objective of assuring that persons with inappropriate records or characters inconsistent with our corporate culture and ethics are identified and eliminated from the hiring process.		
All of our employees, vendors, contractors, and business partners have been made aware of our zero-tolerance policies related to fraud and are aware of the appropriate steps to take in the event that any evidence of possible fraud comes to their attention.		
We have a rigorous program for communicating our fraud-prevention policies and procedures to all employees, vendors, contractors, and business partners.		
We have policies and procedures in place for authorization and approvals of certain types of transactions and for certain values of transactions to help prevent and detect the occurrences of fraud.		
Our performance measurement and evaluation process includes an element specifically addressing ethics and integrity as well as adherence to the Code of Conduct.		
All new hires must undergo rigorous ethics and fraud-awareness and fraud-prevention training.		
All employees must attend periodic (at least annual) ethics and fraud awareness and fraud-prevention training, and the effectiveness of this training is affirmed through testing.		
Terminated, resigning, or retiring employees participate in an exit interview process designed to identify potential fraud and vulnerabilities to fraud that may be taking place in our organization.		
We review the above fraud-prevention mechanisms on an ongoing basis, document these reviews and take necessary action.		

Appendix D

A Brief Note on COSO Internal Control Framework

COSO[10] internal control framework defines Internal Control as an *integral process* that is operated by an entity's management and personnel and is *designed to address risks* and to provide reasonable assurance that in pursuit of entity's mission, the following general objectives are achieved:

- executing orderly, ethical, economical efficient and effective operations;
- fulfilling accountability obligations;
- complying with applicable laws and regulations;
- safeguarding resources against loss, misuse and damage

Internal control is not a single measure but a series of prescriptions of dos and don'ts that touch every activity of the organization. In that sense it is an integral part of the organization. Also, internal control is not something which is separate from the people who operate them. It is part of the roles and responsibilities of the persons working in the entity. As all entities exist for a purpose, the basic objective of internal control is to ensure that the entity achieves its mission; in other words, it aims to minimize the risks that the entity may not be able to achieve its mission. Any system of internal control can provide only reasonable assurance as it would be not be economical to provide an absolute assurance. This recognizes the fact that there are costs associated with any internal control and such costs should not exceed benefit derived from it. Moreover, excessive controls may result in employees circumventing them and, they could also result in delays and inefficiencies in operations.

Apart from ensuring ethical, efficient, economical and effective operations, one of the main objectives of internal control in public sector is to safeguard resources which are acquired with public money. With the extensive use of Information Technology in many government entities, internal controls related to IT have also assumed great deal of importance. Managers of entities where IT is used should be aware of risks of poor controls in IT systems, particularly where they deal with payroll, procurement, stores, etc.

Internal control system exists to help organizations to meet their goals and objectives. They enable management to deal with the changes in internal and external environments. They also promote efficiency, reduce risk of loss, and help ensure financial statement reliability and compliance with laws and regulations (COSO Internal Control Framework). COSO Framework for

[10] Committee of Sponsoring Organizations

internal control system consists of five interrelated and equally important components:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

The *control environment* sets the tone of an organization, influencing the control consciousness of its staff. It is the foundation for all other components of internal control, providing discipline and structure. This is, as already pointed out, determined by the management. Elements of control environment include:

- Personal and professional integrity and ethical values of the organization;
- Commitment to competence;
- The 'tone at the top';
- Organizational structure; and
- Human resource policies and practices;

Risk assessment is the process of identifying and analyzing relevant risks to the achievement of entity's objectives and determining the appropriate response. Elements of risk assessment are:

Risk identification*:* The entity must identify risks that any of its stated objectives would not be achieved. To illustrate, an entity involved with conducting an examination, evaluating the answer papers and declaring results should assess the risk that any of these activities is not done properly. Once a risk (e.g. risk of breach of confidentiality of question paper) is identified, the entity should provide adequate internal control measures to reduce / eliminate the risk.

Risk evaluation*:* Risk evaluation involves assessing the significance of the risk (in terms of its gravity) and the possibility of the risk actually materializing. This requires the organization to categorize risks as high, medium or low based on some judgment. The idea is for the organization to address the high category risks. In the above example, significance and possibility of risk i.e. breach of confidentiality would be considered very high.

Risk assessment*:* Risk assessment requires the entity to understand how much risk it is able to take. This is important because any risk mitigation comes at a cost. Sometimes, it is possible to transfer the risk to a third party. In the above case, the department responsible for conducting the examination cannot simply afford the risk of a leak of question paper. It severely affects its reputation besides compromising its credibility and causing inconvenience to the students / candidates.

Developing a response: After having identified the risks, evaluated and assessed them, the entity must develop a response to mitigate (reduce / eliminate) the risk. Appropriate response could involve *transfer, tolerate, terminate or treat* the risk. Obtaining insurance is an example of transferring the risk. Sometimes, it may be better to live with a risk that is too expensive to treat. Where the risk is too big, it might be better to terminate the activity altogether. This option may not always exist in government sector as there are obligations to society that have to be met irrespective of risks. Lastly, which is in most cases, the entity would like to treat the risk by adopting suitable control activities. In the above illustration, the department would take many precautions (controls) e.g. firstly this work would be handled at a fairly senior level by a very few persons; final selection of questions, printing of question papers, their transmission, custody and so on will be clearly demarcated so that responsibility for any breach of confidentiality is easily identified. The table below gives some examples of risk handling:

Risk	Response	Action
Breach of confidentiality of a question paper	Treat	a) Handled by a very few selected individuals; and b) roles and responsibilities clearly established.
Fire	Partly Treat Partly Transfer	Ensure that a) there are no combustible material in the premises; b) the electrical wiring is proper; Take Fire Insurance
Financial risk in operating commercial infrastructure venture such as a toll bridge	Transfer	Sign a Build Operate Transfer agreement which passes the risk to private partner
Risk of use of government resources (stationery) for personal use	Tolerate	Expenses on controlling this would be disproportionately large compared to corresponding benefit.
Government is obliged to provide services that are not provided by private enterprises due to high risk such as social and physical infrastructure; therefore, this option does not practically exist in government.	Terminate	

Control activities are the policies and procedures established to address risks and to achieve the entity's objectives. There are four types of controls.

- *Prevent Control:* This type of internal control would prevent a risk from occurring. An example of this would be barring the physical access to cash chest or the place from where cashier operates.
- *Corrective Controls:* These controls are designed to correct undesirable outcomes which have been realised. They provide a route of recourse to achieve some recovery against loss or damage. An example of this would be design of contract terms to allow recovery of overpayment. Contingency planning is an important element of corrective control as it is the means by which organisations plan for business continuity / recovery after events which they could not control.
- *Directive Controls:* These controls are designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided - typically associated with Health and Safety or with security. Examples of this type of control would be to include a requirement that protective clothing be worn during the performance of dangerous duties, or that staff be trained with required skills before being allowed to work unsupervised.
- *Detect Control:* Detect controls are measures that would point to misdeeds through reconciliation / review. Any kind of reconciliation (bank reconciliation), post audit, etc. would fall under this category as they help detect if something had gone wrong.

As a general rule, preventive controls are more expensive than detective controls. Any good system of internal control should have good mixture of the two. Also, it would not be too prudent to place excessive reliance on prevent control to the exclusion of detect control because once a prevent control is compromised, there is no way to detect that an illegal act has or is occurring.

To be effective control activities must be:

- Appropriate
- Function consistently
- Cost effective
- Comprehensive
- Directly relate to control objectives

Some examples of control activities are:

Authorizations and approvals: Authorization is the principal means of ensuring that only valid transactions and events are initiated as intended by the management. Authorization procedures must be well documented and clearly communicated to managers and employees. These should include specific conditions and terms under which authorizations are to be made.

Segregation of duties: To reduce the risk of error, waste, or wrongful acts and the risk of not detecting them, no single individual or team should control all key stages of transaction or event. Therefore, duties and responsibilities should be so assigned to a number of individuals that there are enough checks and balances. Notwithstanding separation of duties, collusion can still take place, which can reduce or destroy the effectiveness of this internal control. A common place example of this internal control is the segregation of duties of cashier and accountant; and that of stores clerk who accounts for receipts and issues and the store keeper who physically handles receipts and issues. A small organization may have too few employees to implement this control. In such cases, the management should be aware of the risks and compensate them in some other manner e.g. enhanced supervision, rotation of employees, and so on.

Control over access to resources and records: Restricting access to resources to authorized individuals reduces the risk of loss or misuse of resources. All assets must be protected against loss and misuse by implementing this control. Facilities such as a photocopier, telephone, internet, vehicle, etc. also require protection against improper use.

Verifications: Transactions or events (receipt of goods supplied or cash balance at the end of day) are verified to ensure correctness and validity. Personal records / service books are periodically verified to ensure their correctness.

Reconciliations: This is one of the most commonly used and effective detect control measure in any organization. Reconciliation of one set of records with another (the DDO’s accounts with Accountant General’s records, own cash book with bank statement).

Reviews and post audit play an important role in ensuring that activities have taken place in accordance with the intents and objects of management. A review of financial statements can reveal if there have been any discrepancies pointing to wrongdoing. A procurement process can be post audited to make sure that it complies with all the regulations.

Supervision: Supervision (assigning, reviewing, approving and guiding, training) is an important and high level internal control. This is something that is done at different levels of management periodically.

Information and communication are essential to realizing all internal control objectives. ‘Management’s ability to make appropriate decisions is affected by (appropriate, timely, current, accurate and accessible) information’. Effective communication should flow down, across and up the organization, through all components and the entire structure

C: Detecting Fraud

Despite strong preventive mechanisms there will always be a possibility of the potential fraudster circumventing the controls to indulge in the perpetration of fraud. Moreover, it is practically impossible to prevent all types of fraud. Nor would it be cost effective. Therefore, it is important that we are able to establish sound systems to detect instances of fraud at the earliest.

One of the strongest deterrents to fraud is the perception that effective detect controls are in place. Combined with preventive controls, detective controls enhance the effectiveness of an antifraud program by providing evidence that preventive controls are working as intended and identifying fraud if it occurs.

Detect controls provide evidence that fraud has occurred, or is occurring. Although they are not by themselves intended to prevent fraud, a strong and effective detect control actually prevents fraud from occurring as the certainty of detection (fraud being found out) decreases the incentive to commit fraud. Detect controls are generally also more economical. A proper audit trail, record of logging into system (in case of computerized systems), surveillance cameras, etc. have tremendous impact on controlling fraud.

In order to be able to detect a fraud, the concerned staff should be familiar with the likely frauds and the indicators that would point to the fraud. They should be sensitized to fraud indicators so that they are able to trigger closer examination of evidence to establish fraud. Suspicious behaviour (such as staying late beyond office hours or attending office on holidays for no apparent reason), unusual events, etc. should raise alarm.

The following are some common ways of a fraud being detected:

a. Normal operation of control procedures

b. Suspicion

c. Accident

d. Internal/ external audit

e. Confessions

f. Third party information

Three important fraud detection methods are

a. an anonymous reporting (whistleblower / hotline) mechanism;

b. internal auditing; and

c. process related controls specifically designed to detect fraudulent activity viz. reconciliations, independent reviews, physical inspections/counts, analyses, and audits.

Given below are some questions that the department / organization might like to ask itself to check if the detection practices are adequate. A more detailed score card to assess effectiveness of detect controls is given in Appendix E at the end of this section.

Check List of Questions

Whether your organisation:

- has a well publicised telephone hotline, email and freepost address to which the public can report cases of suspected fraud;
- uses techniques proactively to detect cases of suspected fraud such as in-depth investigative work into "hotspot" areas, data matching exercises, data mining and neural networks as appropriate;
- works with others to tackle fraud.

C.1 Set up and encourage the use of hotlines to detect fraud

'Hotlines prove to be one of the most effective ways of obtaining input on undesirable behaviour. Recent research suggests that at least 25 percent of the frauds which are discovered come to light because of reports via hotlines. And Association of Certified Fraud Examiners reports that over 34 percent of fraud comes to light as a result of tips. These figures are clear evidence that in general, hotlines are extremely valuable tool in (an organization's) anti-fraud program. In particular, anonymous hotlines mean that potential whistleblowers need not be afraid of reprisals from within the (organization).'

A Survey into Fraud Risk Mitigation in 13 European Countries – Ernst& Young

A hotline has to be at a fairly aggregated level – that is at the government level (Vigilance Commission) or at the department level. In other words, hotlines would not be feasible at individual office level. Moreover, having hotline at the office level would discourage the potential whistleblower as he would not be confident of the office's objectivity and fairness in dealing with the report as it involves the same office / officers.

Hotlines can be a cost effective way of obtaining from staff and the public details of possible cases of fraud which can be assessed and investigated further. Referrals may come from

a. Staff who have carried out checks on transactions and suspect a fraud.

b. Members of the public may contact the department about their suspicions.

c. Fraud investigators may develop their own intelligence by following leads on existing cases where there may be links to other frauds.

The employees should be encouraged to report any delinquency that he/she has observed in any of the colleagues without any fear or favour either to their supervisors, to internal audit or use the hotline. It is one of the employees who would be able to identify any irregularity or fraud taking place since the fraudster would perhaps be a colleague or an outsider dealing with the employee. In many cases, if the fraud is perpetrated by a superior, the lower level employee would possibly be hesitant to openly air his suspicion. The employees should therefore be encouraged to use the hotline to report any irregularity with the assurance that their identity would remain confidential, if disclosed. There should be a provision to report anonymously. However, the organization should have a proper system of scrutinizing the reports to establish their authenticity. It should ensure that the system is not used for settling personal scores or to malign and harass colleagues. For this purpose, the investigation into the reports files through hotline should also take place discreetly.

The organization should take the following measures:

- Set up a toll-free telephone number, with alternative means of contacting the department including an email and freepost addresses;
- Publicize the telephone number, contact details, email address, postal address through the organization's website, leaflets and posters, etc.
- Indicate the information that is useful in a referral, including the types of frauds that the department is particularly interested in hearing of and how the department will deal with the information provided;
- Give assurance that particulars of the person reporting fraud would be strictly kept in confidence. For this, the organization must develop necessary procedures so that the identity of the person reporting fraud is not disclosed under any circumstances;
- Develop a standard form to report fraud so that the person making the referral into provides as much relevant information as possible. An electronic version of the form can be included on a website, which can be completed and submitted anonymously online; and
- Provide feedback on action taken.

Hotlines should be evaluated at regular intervals, for example, analyzing the number and type of referrals received, what has happened in each case, and over all results.

A hotline should allow the caller to remain anonymous, thereby minimizing fears of reprisal from reporting such activities. This is one of the keys to a successful hotline. Another key is assurance that the notification will result in some action being taken. The hotline should be promoted with educational materials provided to stakeholders, employees, customers, and vendors, all of whom can provide valuable information from a variety of reliable sources. In addition, the management should deal swiftly with any attempts to bring harm to whistleblowers. A culture of over-reporting and effective and swift handling should be encouraged.

A well-designed hotline typically includes the following features:

- **Confidentiality**. All matters reported via the hotline are treated confidentially. Hotline operators inform callers that their concerns will be reported only on a "need to know" basis and that relevant safeguards are in place to ensure that such confidentiality is maintained. Hotline operators notify callers if the confidentiality of the matter is subject to any legislative limitations.
- **Anonymity**. The organization's protocols allow for the anonymous submission and resolution of calls. For instance, callers who wish to

remain anonymous are given a case tracking number that they can later use to provide additional details related to their question or allegation and/or check the status or outcome of their call.

- **'Real Time' Assistance**. The hotline is designed to provide an immediate, "live" response to a call to facilitate thorough and consistent treatment of a caller's question or concern as well as to provide immediate guidance. Thus, hotline operators need to be appropriately qualified, trained, and, in some situations, authorized to provide advice.
- **Data Management Procedures**. The hotline operator uses consistent protocols for gathering relevant facts and managing the hotline calls.
- **Follow-up on Non-retaliation**. The organization's protocols allow for following up with employees periodically after the hotline case has been closed (e.g., at one-, three-, and six-month intervals) to ensure that reporting employees have not experienced retaliation. The company encourages the employees to report any instances of retaliation and takes swift action against those who do retaliate.
- **Prominent Communications**. The organization publicizes its hotline prominently. Such communications may include, among others, (1) describing the hotline within the code of conduct and other key company publications and training; (2) displaying the hotline telephone number on posters, banners, wallet cards, screen savers, telephone directories, or desk calendars; and (3) communicating mini case-studies based on hotline calls to employees (e.g., in newsletters, training programs, or intranet sites) to demonstrate that the organization values hotline calls and is able to provide assistance to those who use the hotline.

A Sample Whistle Blowing Policy is given at Appendix F at the end of this section.

Whistle Blower Protection

Though there is no formal Act for protecting the Whistleblowers as there in the USA (the Qui Tam Act), the government of Andhra Pradesh in the year 2005, issued an order, GO No.479, empowering the AP Vigilance Commission to give protection to the Whistle Blowers on the similar lines as those given by the Central Vigilance Commission. GoAP authorized the APVC to receive written complaints or disclosure on any allegation of corruption or of misuse of office by any employee of the State government or of any corporation established by or under any State Act, government Companies, Societies or local authorities owned or controlled by the state government. The order further instructs the APVC to ensure the confidentiality and accuracy of the information disclosed by the whistleblower while protecting his identity. If any person is aggrieved by any action on the ground that he is being victimized due to the fact that he had filed a complaint or disclosure, he may seek redressal from the APVC by filing an application with the latter. The APVC shall give suitable directions to the concerned public servant or the public authority as the case may be.

Deal with information received through hot line effectively

The organization should ensure that it has a system for prompt, competent, and confidential review, investigation, and resolution of allegations involving potential fraud or misconduct received by way of tips from employees, customers or vendors (through hotline). Protocols for the top management's involvement in such cases which will vary depending on the nature, potential impact, and seniority of persons involved should be clearly defined and communicated to concerned officers.

The investigation and response system should include a process for:

a. Categorizing issues.

b. Confirming the validity of the allegation(s).

c. Defining the severity of the allegation(s).

d. Escalating the issue or investigation when appropriate.

e. Conducting the investigation and fact-finding.

f. Resolving or closing the investigation.

g. Listing types of information that should be kept confidential.

h. Defining how the investigation will be documented.

C.2. Identify and act upon Red Flags (Fraud Indicators)

The term ***"red flag"*** *refers to anomalies, unusual events, a signal that informs or indicates, announces or communicates that something is different from the norm or the expected activity*

Although poor management's decisions or negligence may give rise to possible indications of fraud, the difference between fraud and negligence is a fine line called intent. What fraud indicators/red flags can do is to point the way for further detailed inquiry.

Asian Organization of Supreme Audit Institutions (*ASOSAI)*

Proactive fraud detection involves aggressively targeting specific types of fraud and searching for their indicators, symptoms or red flags. Early fraud detection is critical because the sizes of most frauds increase geometrically over time as perpetuators gain confidence that their schemes are not being detected.

CIMA's Fraud Risk Management makes a distinction between warning signs and red alerts. While red alerts are specific events, warning signs are those which predispose an organization to the risk of fraud. Further it also categorizes the warning signs into cultural issues, management issues, employee issues, process issues and transaction issues, which is interesting.

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. Some fraud indicators i.e. red flags are:

Staff / Officers

- 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 or 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.
- Has genuine financial need.

- Employees with outside business interests or other jobs;
- Managers bypassing subordinates;
- Subordinates bypassing managers;

Other areas

- Too many outstanding Abstract Contingent Bills / advances.
- Too many outstanding audit queries / objections;
- Delayed or incorrect utilization certificates;
- Key documents missing (e.g. invoices, contracts).
- Documentation that is photocopied or lacking essential information.
- Missing expenditure vouchers and official records.
- Excessive variations to budgets or contracts.
- Excessive movements of cash or transactions between accounts.
- Numerous adjustments or exceptions.
- Overdue pay or expense advances.
- General ledger out of balance.
- Duplicate payments.
- Unauthorised changes to systems or work practices.
- Post Office boxes as shipping addresses.
- Lowest tenders or quotes passed over with minimal explanation recorded.
- Single vendors.
- Unclosed but obsolete contracts.
- High staff turnover rates in key controlling functions.
- Chronic understaffing in key control areas.
- Frequent management overrides of internal control.
- Refusals to produce files, minutes or other records;
- Increased employee absences;
- Figures, trends or results which do not accord with expectations;
- Bank reconciliation's are not maintained or can't be balanced;
- Multiple cash collection points;
- Remote locations;
- Large outstanding bad or doubtful debts;
- Placing undated/post-dated personal cheques in petty cash;
- Large sums of unclaimed money;

- Large sums held in petty cash;
- Excessive control of all records by one officer;
- Personal creditors appearing at the workplace;

C.3. Use statistical and ICT tools in the detection of fraud

Use of ICT has brought about a revolutionary change in fraud detection. Effective detection tools can be used to discover fraud at its nascent stage of occurrence to help confine the extent of loss to the Department. Tools like data mining, data matching and neural networks can be used to identify the relationships and patterns between different datasets and note any discrepancies or irregularities that would evolve into fraud. Standardization of databases, however, is a prerequisite for the successful ICT intervention.

It must be remembered, however, that we can seldom be certain, by statistical analysis alone, that a fraud has been perpetrated. Rather, the analysis should be regarded as alerting us to the fact that an observation is anomalous, or more likely to be fraudulent than others, so that it can then be investigated in more detail. One can think of the objective of the statistical analysis as being to return a *suspicion score* (where we will regard a higher score as more suspicious than a lower one). The higher the score is, then the more unusual is the observation or the more like previously fraudulent values it is.

Data matching

Data matching involves computerized scanning of data held in different data files either within the same organization or in different organizations. It can be used by management for a range of purposes including detecting potential fraud. With increasing computer power, data matching across files is possible on a very large scale.

Data sharing allows entities that make payments—to contractors, vendors, or participants in benefit programs—to compare information from different sources to help ensure that payments are appropriate. For government agencies, data sharing can be particularly useful in confirming initial or continuing eligibility of participants in benefit programs and in identifying improper payments that have already been made.

To help focus resources on the matches which indicate possible fraud, data matching software:

- Highlights the highest priority matches;
- Allows users to filter only those matches that meet investigators' criteria for investigation;
- Explains the importance of each match type and protocols for sharing information between matched bodies.

Data matching exercises should comply with the provisions of the Data Protection legislation. It should in any case be ensured that the data is:

- Fairly and lawfully processed;

- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;
- Processed in line with the individual's rights;
- Secure; and
- Not transferred to other without adequate protection.

The Department for Work and Pensions, U.K. has developed a Matching Intelligence Data Analysis Service which produces a series of data matches between their benefits and information systems as well as with other departments. It has access to over 100 different types of matches which results in around 300,000 matches per year, identifying potential fraud and error.

The Audit Commission's National Fraud Initiative is the largest data matching exercise in Europe in relation to fraud. Driver and Vehicle Licensing Agency also uses data matching to detect vehicle excise duty evasion.

Australian experience: The parallel data-matching software makes use of tax file numbers and permits income records to be compared with payment record of various benefit providing departments. The program permits anomalies in payments to be identified for further investigation, and also permits the identification of individuals who are entitled to receive benefits which they have not claimed. In the year 1996-97, the program resulted in savings of $A 157 million for two departments.

Data Mining

Data mining is the process of selecting, exploring and modeling large amounts of data to reveal previously unknown patterns, behaviours, trends or relationships which may help to identify cases of fraud. Because of the large amount of data that needs to be analysed, specialist computer software is used which usually contains a range of data mining tools. A number of software companies have developed such products.

Data mining can be a powerful way of interrogating data and revealing anomalies that would not be revealed by other techniques. However, to enable it to function most effectively, staff need to be trained in the use of the software, and to gain experience in selecting the most appropriate tools to scrutinize the data and in following up anomalies to detect cases of fraud.

Neural networks

A neural network is intended to simulate the way in which a brain processes information, learns, and remembers. A neural network is initially “trained” or fed large amounts of data and rules about data relationships (for example, “a person’s grandfather is older than that person’s father”). Neural networks "learn" by comparing new data with historical data and can be used to detect patterns that are difficult, and sometimes impossible, to detect without computer intervention in large volumes of data. The more data a neural network processes the better it performs (i.e., the better it identifies the characteristics of potentially fraudulent payments). Based upon this knowledge, neural networks automatically alter their analytical processes to produce more accurate detection results.

Neural networks are computer based multiprocessing systems which are designed to connect data from multiple sources to identify structures and patterns and exceptions to an identified structure or pattern. The ability of neural networks to identify patterns of activity and exceptions to a pattern that may be associated with fraud, gives organisations an ability to focus their detective efforts on these exceptions.

One of the problems of using these techniques more widely in the public sector is that the data may not be held in a way that lends itself to such analysis. The move towards providing services online may change this and allow real time analysis of transactions through the Department's websites using some of these techniques.

Un-programmed checks

'Sometimes the perpetrators of frauds make allowance for routine internal audits and design their activities to avoid detection by scheduled checks. The predictability of scheduled checking of captured transactions can be a problem. For example, checks may miss shortfalls in stock or valuables that have been temporarily made up to make it appear that all is in order.

To address this, in addition to frequent scheduled audits, random checks should be conducted. Organizations should consider the level of fraud risk and the potential losses involved when determining the frequency and intensity of such checks.

Data Analysis

In addition to detective process controls, organizations may be able to effectively use data analysis and continuous auditing techniques to detect fraudulent activity. Data analysis uses technology to identify anomalies, trends, and risk indicators within large populations of transactions. Data analysis allows users to identify relationships between people, organizations, and events.

Proactive consideration of how certain fraud schemes may result in identifiable types of transactions or trends enhance an organization's ability to design and implement effective data analysis. Data analytics can also be used to cost-effectively ensure that other fraud-prevention and detection controls in place are effective.

Continuous Auditing

Continuous auditing is the use of data analytics on a continuous or real-time basis, thereby allowing management or internal auditing to identify and report fraudulent activity more rapidly. For example, a Benford's Law analysis[11] can be used to examine expense reports, general ledger accounts, and payroll accounts for unusual transactions, amounts, or patterns of activity that may require further analysis. Similarly, continuous monitoring of transactions subject to certain flags may promote quicker investigation of higher-risk transactions.

Routine verification

All accounts, bills, invoices and other sundry demands for payment received by an organisation must be checked. This process should involve at least two people. One should verify the expenditure was incurred. The other should ensure that the expenditure was properly authorised in the first place and then authorise payment. The same person should never incur expenditure and authorise the payment of a resulting account.

There are dangers in setting threshold amounts below which transactions need not be properly verified. Organisations are vulnerable to the practice of 'skimming', where fraudsters routinely make false small claims for amounts over time.

Credit cards numbers can be used to conduct many small, fraudulent transactions. These appear on statements but can go undetected as they get below an organisation's "money radar". That is, they are for amounts less that those for which the organisation insists on the provision of documentary verification.

False pro-forma invoices can also siphon away assets. Operators of this type of fraud send apparently genuine invoices to organisations. They hope to exploit inadequate internal verification systems and so receive payments fraudulently. You need to make sure that documents that appear to be genuine demands for payment for goods or services received cannot be routinely paid without verifying that the goods or service were provided.

Refunds and nil-amount transactions also present risks. All such instances should be checked and authorised by a second officer. This involves using

[11] Benford's Law is based on a peculiar observation that certain digits appear more frequently than others in data sets. *The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data, Cindy Durtschi, William Hillison and Carl Pacini, Journal of Forensic Accounting 1524-5586/Vol V(2004) provides an excellent exposition of Benford's Law*

what are called exception systems. These systems produce reports detailing the time, place and operator whenever an exceptional transaction takes place. Unusually high numbers of refunds and cancelled transactions may indicate there is a problem. A background system to monitor these kinds of trends is a very useful tool if your organisation processes lots of transactions.

***Note**: Strategic Fraud Detection: A Technology-based Model – Conan C Albrecht and W Steve Albrecht, Rollins Centre for eBusiness provides a very good guidance on adopting a computer based approach to proactively detecting fraud.*

C.4. Institute an effective internal audit system

Internal auditing should provide assurance that fraud prevention and detection controls are sufficient for identified fraud risks, and ensure that the controls are functioning as designed. Internal auditing should also be alert for incidences of actual fraudulent activity and may be responsible for initial or full investigation of suspected fraud schemes.

Although management and those charged with governance are responsible for assessing fraud risks and designing internal controls to prevent, detect, and mitigate the fraud risks, internal auditors are an appropriate resource for assessing the effectiveness of what management has implemented. The importance an organization attaches to its internal audit function is an indication of the organization's commitment to effective internal control. An internal audit department's charter should direct the role of internal auditing in an antifraud program.

Internal auditors should consider the organization's assessment of fraud risk when developing their annual audit plan and periodically assess management's fraud-detection capabilities. They should also interview and regularly communicate with those conducting the assessments, as well as others in key positions throughout the organization, to help them assess whether all fraud risks have been considered. When performing engagements, internal auditors should devote sufficient time and attention to evaluating the design and operation of internal controls related to preventing and detecting significant fraud risks. They should exercise professional skepticism when reviewing activities to be on guard for the signs of potential fraud. Potential frauds uncovered during an engagement should be treated in accordance with a well-defined response plan consistent with professional and legal standards.

Effective internal audit departments are adequately funded, staffed, and trained, with appropriate specialized skills given the nature, size, and complexity of the organization and its operating environment. Internal auditors should be aware of and trained in the tools and techniques of fraud detection, response, and investigation as part of their continuing education program. The department should be independent (authority and reporting relationships), have adequate access to the audit committee, and adhere to professional standards.

However it is important to note that Internal Audit is neither a substitute for management ownership of risk nor a substitute for an embedded review system carried out by the various staff, who have executive responsibility for the achievement of organisational objectives.

Appendix E

Fraud Detection Scorecard
(to assess effectiveness of detective measures)

To assess the strength of your organization s fraud-detection system, carefully assess each area below and score the area, factor, or consideration as either:

- 🔴 indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level.
- 🟡 indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level.
- 🟢 indicating that the area, factor, or consideration is strong and fraud risk has been reduced at least to a minimally acceptable level.

Each area, factor, or consideration scored either red or yellow should have a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud-detection Area, Factor, or Consideration	***Score***	***Notes***
Our fraud-detection policies include communicating to employees, vendors, and stakeholders that a strong fraud-detection system is in place, but certain critical aspects of these systems are not disclosed to maintain the effectiveness of hidden controls.		
We use mandatory vacation periods or job rotation assignments for employees in key finance and accounting control positions.		
Our fraud-detection mechanisms place increased focus on areas in which we have concluded that preventive controls are weak or are not cost effective.		
We focus our data analysis and continuous auditing efforts based on our assessment of the types of fraud schemes to we are susceptible.		
We take steps to assure that our detection processes, procedures, and techniques remain confidential so that ordinary employees and potential fraud perpetrators do not become aware of their existence.		
We have comprehensive documentation of our fraud-detection processes, procedures, and techniques so that we		

Fraud-detection Area, Factor, or Consideration	***Score***	***Notes***
maintain our fraud-detection vigilance over time and as our fraud-detection team changes.		
Our detective controls include a well-publicized and well-managed fraud hotline.		
Our fraud hotline program provides anonymity to individuals who report suspected wrongdoing.		
Our fraud hotline program includes assurances that employees who report suspected wrongdoing will not face retaliation. We monitor for retaliation after an issue has been reported.		
Our fraud hotline has a multilingual capability and provides access to a trained interviewer 24 hours a day, 365 days a year.		
Our fraud hotline uses a case management system to log all calls and their follow-up to resolu`tion, is tested periodically by our internal auditors.		
Our information systems/IT process controls include controls specifically designed to detect fraudulent activity, as well as errors, and include reconciliations, independent reviews, physical inspections/counts, analyses, audits, and investigations.		
Our internal auditors participate in the fraud risk assessment process and plan fraud-detection activities based on the results of this risk assessment.		
Our internal audit department is adequately funded, staffed, and trained to follow professional standards, and our internal audit personnel possess the appropriate competencies.		
Our internal audit department performs risk-based assessments to understand motivation and where potential manipulation may take place.		
Our internal audit personnel are aware of and trained in the tools and techniques of fraud detection, response, and investigation as part of their continuing education program.		
We use data analysis, data mining, and digital analysis tools to: (a) identify hidden relationships between people, organizations, and events; (b) identify suspicious transactions; (c) assess the effectiveness of internal controls; (d) monitor fraud threats and vulnerabilities; and (e) consider and analyze		

Fraud-detection Area, Factor, or Consideration	***Score***	***Notes***
large volumes of transactions on a real-time basis.		
We use continuous auditing techniques to identify and report fraudulent activity more rapidly, including Benford's Law analysis to examine expense reports, and payroll accounts for unusual transactions, amounts, or patterns of activity that may require further analysis.		

Appendix F

Sample Whistle-Blowing Policy

Introduction

This whistle-blowing policy provides a procedure which enables employees to raise concerns about what is happening at work, particularly where those concerns relate to unlawful conduct, financial malpractice or dangers to the public or the environment. The object of this policy is to ensure that concerns are raised and dealt with at an early stage and in an appropriate manner.

This organisation is committed to its whistle-blowing policy. If an employee raises a genuine concern under this policy, he or she will not be at risk of losing their job, nor will they suffer any form of harassment as a result. As long as the employee is acting in good faith and in accordance with this policy, it does not matter if they are mistaken.

How the Whistle-Blowing Policy differs from the grievance procedure

This policy does not apply to raising grievances about an employee's personal situation. These types of concerns are covered by the organisation's grievance procedure. The whistle-blowing policy is primarily concerned with issues where the interests of others or of this organisation itself are at risk.

Protecting the Employee

This organisation will not tolerate harassment or victimisation of anyone raising a genuine concern under the whistle-blowing policy. If an employee requests that their identity be protected, all possible steps will be taken to prevent the employee's identity becoming known. If the situation arises where it is not possible to resolve the concern without revealing the employee's identity (e.g. if the employee's evidence is needed in court), the best way to proceed with the matter will be discussed with the employee.

Employees should be aware that by reporting matters anonymously, it will be more difficult for the organisation to investigate them, to protect the employee and to give the employee feedback. Accordingly, while the organisation will consider anonymous reports, this policy does not cover matters raised anonymously.

How the matter will be handled

Once an employee has informed the organisation of his or her concern, the concerns will be examined and the organisation will assess what action should be taken. This may involve an internal enquiry or a more formal investigation. The employee will be told who is handling the matter, how they can contact him/her and whether any further assistance may be needed. If the employee has any personal interest in the matter, this should be declared by the employee at the outset. If the employee's concern falls more properly within the grievance procedure, then they will be told this.

How to raise a concern internally

Step 1

If an employee has a concern about malpractice, he or she should consider raising it initially with their line manager. This may be done orally or in writing.

An employee should specify from the outset if they wish the matter to be treated in confidence so that appropriate arrangements can be made.

Step 2

If an employee feels that they are unable to raise a particular matter with their line manager, for whatever reason, they should raise the matter with their head of office.

Step 3

If these channels have been followed and the employee still has concerns, or if the employee feels that the matter is so serious that he cannot discuss it with any of the above, they should discuss it with the head of department.

Matters raised maliciously

Employees who maliciously raise a matter that they know to be untrue will be subject to the disciplinary action.

D: Investigate and deal effectively with detected cases of fraud

Once a fraud is detected, it is essential that it is investigated in the most professional, objective and timely manner possible. Investigations are to be undertaken by trained staff and have to be compliant with the legal provisions.

Where fraud has occurred, the department or agency should consider:

- stopping the fraud at the earliest opportunity and looking at whether weak controls have been exploited which need to be tightened up;
- whether to prosecute the case criminally or departmentally;
- collect arrears and penalties to ensure that the economics of the crime are undermined and to deter others.

While ordinary cases of misappropriation may be handled with relatively less expertise, more serious types of fraud involving complex modus operandi require special skills and knowledge. Since in such cases, either the CID or the Economic Offences wing of CID would be in charge of investigation, the staff of these organizations should be provided training in forensic audit techniques. It is also a desirable practice for these organizations to recruit specialists in computers, accounts, audit, etc. to assist in fraud investigations.

Check List of Questions

Whether your organisation (or the investigating agency, as the case may be):

- tracks the progress of individual investigations;
- has sufficient investigative staff with the essential technical knowledge and experience;
- imposes appropriate sanctions on fraudsters such as fines or, other penalties, or criminal prosecution in appropriate cases;
- seeks to recover the amounts lost from fraud; and
- evaluates the effectiveness of sanctions.

D.1. Equip the organization with the right skills to undertake professional investigation of the fraud that has been detected

Normally initially discovered fraud only reveals a single instance of fraud or anomaly – the proverbial tip of the iceberg. The Department would have to go into the instance of fraud methodically to uncover the whole truth. This requires special skills such as forensic auditing. The internal audit department as also the specialized departments should have competent staff for systemic and scientific investigation. They should identify a range of training courses 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, forensic audit methods, etc.).

In the government, investigation of serious cases of fraud is undertaken by either CID or Anti-Corruption Bureau. The individual departments have very little role in investigation after a fraud has been reported to police. Firstly, the staff of these departments should be provided training in specialized skills and knowledge to the extent feasible. Secondly, they should recruit specialists / experts in computer systems, accounting methods, banking, etc. to assist the general investigating teams on need basis,.

D.2. Respond effectively to fraud when it occurs

Department must ensure that the actions are taken as per the organisation's Fraud Response Plan. Depending on the significance of the fraud, an effective response to fraud involves some or all of the following:

a. Head of Office / Department should provide the leadership and direction for fraud investigation.

b. The Head of Office should report the matter at once to the Accountant General and through proper channel to the Head of Department.

c. Institute departmental proceedings at the earliest possible moment against all the government servants involved in any loss sustained by government on account of fraud, embezzlement or any similar offence.

d. It should be ensured that charges are framed by the disciplinary authority as per prescribed procedures and action is completed expeditiously observing the prescribed procedures to ensure that there are procedural infirmities.

e. Whenever there is a reasonable ground for suspecting that a criminal offence has been committed in respect of public monies or properties, the matter should at once be reported to the police.

f. If the quantum of money involved is very large or the case involves complex modus operandi, the matter should be taken up with Secretariat Department for being referred to CID for investigation.

g. A departmental audit should be initiated to establish the instances and amounts of misappropriation.

h. Set up a mechanism to report on progress of the investigation to appropriate senior levels of management.

i. Ensure 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.

j. Set up adequate measures to protect the public confidence throughout the investigation process particularly when issuing statements to the media.

k. Initiate 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 for reducing the risk of recurrence.

D.3. *Enforce effective sanctions, including appropriate legal action against people committing fraud*

Where investigations find evidence of fraud, departments will usually seek to impose some form of sanction. The purpose of imposing sanctions is:

- To deter others from carrying out similar types of fraud against the organization;
- Recover the money defrauded and
- Punish the fraudster by imposing a penalty, such as a fine, or confiscating an asset, or by prosecuting them criminally in the courts.

Imposition of sanctions following the investigations demonstrates a non-tolerance of fraud within the Departments and would act as deterrent for potential fraudster. The level of sanctions imposed shall be commensurate to the type and scale of fraud committed. The extent of repeat of offences is a good indicator of whether sanctions were a sufficient deterrent. Continuous monitoring of the effective implementation of sanctions also shall be undertaken.

Fines and other penalties imposed on those committing fraud need to be recovered to ensure that they act as a deterrent. It is important to monitor progress in recovering the fines and penalties involved, including the enforcement of fines imposed by the courts for convicted fraudsters. Although in such cases it is not the departments that collect the fines, they should follow up the matter to see that the fines are actually paid.

Wherever warranted department or agency shall initiate criminal prosecution. Preparing cases to the state of proof required for a criminal prosecution can take a long time and involve significant resources. Decisions on whether to prosecute may depend on whether:

- The case involves a systematic attack on the department's systems and has led to substantial amounts of money being lost;
- There is a history of repeat offences;
- There is sufficient evidence to obtain a conviction; and
- Prosecution will increase the deterrent effect.

These factors need to be balanced against the time and cost of bringing a case to court, and the availability of other forms of sanction which may be more appropriate.

Punitive action - Immediate dismissal upon conviction

An officer who is convicted by a Criminal Court for the offence of misappropriation or fraud should be dismissed from service without waiting for filing of an appeal or its outcome. Such action would be taken notwithstanding suspension of sentence by an Appellate Court. It is not necessary to consult the Public Service Commission (in Andhra Pradesh) for taking action to dismiss the officer on the grounds of conviction in a Court of Law. In the case of an officer who in the meantime has retired, his pension and gratuity should be withheld or where it has already been sanctioned, his pension should be withdrawn. The officer who fails to enforce these instructions promptly, should be held responsible for any loss to the government on account of avoidable payment of subsistence allowance or provisional pension as the case may be

Suspension pending inquiry / investigation

Supreme Court has consistently held that it is the prerogative of the disciplinary authority to place an officer under suspension pending inquiry/investigation/trial and that it shall not be ordinarily interfered with.

The Head of Department should send a full statement of the facts of the case to higher authorities if prosecution results in the discharge or acquittal, or in the imposition of any sentence which appears to be inadequate with a request that further proceedings should be taken up for revision or appeal.

D.4. Monitor and evaluate the effectiveness of sanctions continuously

Department or agency should evaluate effectiveness of sanctions on a continuous basis. Evaluating the effectiveness of sanctions may be difficult task, mainly because of the difficulties in assessing the deterrent effect. In broad terms, the deterrent effect of sanctions will be reflected in whether the amount of fraud has reduced.

The following parameters may be taken as indicators to determine effectiveness of sanctions:

- Number of frauds identified;
- Number of identified frauds with no sanction imposed;
- Number of cases where re-offending has occurred;
- Number of formal cautions given;
- Number of penalty charges imposed;
- Amount raised by imposition of penalty charges;
- Number of cases recommended for criminal prosecution;
- Number of convictions achieved;
- Amount of fraud loss and amount recovered;
- Number of confiscation orders and amount recovered;
- Amount of assets seized from the fraudsters.

D.5. Adopt effective methods for seeking redress in respect of money defrauded.

The recovery of the defrauded money and its return to the provision of services is an integral part of strategic fraud risk management. It can be seen as a deterrent for the fraudsters - that there is no benefit to be gained from fraud.

Investigators may look into the financial matters of the fraudster to provide evidence in the court of law on the benefit derived by the fraudster and seek confiscation order. The means of recovering assets may be achieved either through a criminal process or civil process. Sometimes civil process may be initiated while criminal process is underway. Department should weigh costs and benefits before proceeding in recovering money. So, department should consider

- Evidence that the amounts are stolen and therefore could be recoverable ;
- The prospects of winning the case;
- The value of assets held by the suspected fraudster;
- Whether it will be possible to pursue a civil action whilst a criminal investigation is underway

Recovery from pension

Pension due to an employee, who is charged or held responsible for loss to government by defalcation of public money, stamps, stores or other movable or immovable property, should not be sanctioned. Efforts should be made to recover the loss from last pay, leave salary or pension due to him.

Attachment and forfeiture of the properties of the accused

Whenever a scheduled offence involving the money of the government is committed, the concerned departmental officers should collect the necessary data regarding movable / immovable property of the persons responsible for commission of the offence, so that such properties may be subjected to attachment and forfeiture under the Criminal Law Amendment Ordinance, 1944 which provides that if any person commits any offence punishable under Section 406, 408, 409, 411, 417 and 420 of the IPC or under clause (c) of sub-section (1) of Section 13 of the Prevention of Corruption Act, 1988, the government may, whether or not any court has taken cognizance of the offence, authorize the making of an application to the District Judge concerned for attachment of the money or other property.

The above provision should be used for attaching the properties of the government servant(s) who are found to have misappropriated government money pending the criminal proceedings and eventual confiscation of the property.

Invoking provisions of Revenue Recovery Act

The provisions of Revenue Recovery Act 1864 can be invoked for recovery of the misappropriated amounts or loss caused to the government. Recovery of these sums can be done as if it were arrear of land revenue in accordance with procedure laid down in the A.P. Revenue Recovery Act. It is open to government to file a civil suit for recovery of such sum as a last resort.

Bibliography

1. *Counter Fraud Strategy – Department of Health, Social Services and Public Safety, Northern Ireland, U.K. (October 2005)*

2. *Fighting Fraud: Guidelines for state and local government (November 2002) Independent Commission Against Corruption, New South Wales, Australia*

3. *Good Practice in tackling external fraud – National Audit Office and HM Treasury U.K.*

4. *Managing the Business Risk of Fraud: A Practical Guide (Exposure Draft November 2007) Institute of Internal Auditors, U.S.A.*

5. *Managing the Risk of Fraud – A guide for Managers (May 2003) HM Treasury, U.K.*

6. *The Orange Book – Management of Risk – Principles and Concepts (October 2004), HM Treasury, U.K.*

7. *Fraud Control in Australian Government Agencies – Better Practice Guide, Australia National Audit Office (2004)*

8. *Resource Guide on Fraud – Facts, Lessons Learned and Best Practices, Nassau County Comptroller, State of New York*

9. *Tackling Benefit Fraud – Department of Work and Pensions, Report of the Comptroller and Auditor General, National Audit Office, U.K.(2003)*

10. *Tackling Fraud against the Inland Revenue- Report of the Comptroller and Auditor General, National Audit Office, U.K.(2003)*

11. *Tackling VAT Fraud – A report by Public Accounts Committee, U.K. (2004)*

12. *Good practice in Countering Fraud - Circular issued by Counter Fraud Policy Unit, Health, Social Services and Public Safety, U.K.*

13. *Dealing with Fraud and Corruption – Training Module by International Organization of Supreme Audit Institutions (INTOSAI)'s International Development Initiative*

14. *Fraud Risk Management – A Guide to Good Practice. The Chartered Institute of Management Accountants, U.K.*

15. *Tackling Staff Fraud and Dishonesty: Managing and Mitigating Risks – A Chartered Institute of Personnel and Development (CIPD) and CIFAS, U.K. Guide*

16. *Fraud Risk Management – Developing a Strategy for Prevention, Detection and Response. Advisory, KPMG Forensic.*

17. *Fraud in Governmental and Private Sectors – Sarah A Holmes, Jeffrey W Srtrawser and Sandra T Welch. Journal of Public Budgeting, Accounting & Financial Management*

18. *Strategies to Manage Improper Payments – Executive Guide. General Accounting Office, USA (October 2001)*

19. *Managing Fraud and Integrity Risk - Best Practices Offer Key: Andrew Flaig and Gloria Chang*

20. *Countering Fraud in National Health Service, Counter Fraud and Security Management Service - NHS, U.K.*

21. *Protecting identity information and documents – Guidelines for public sector managers (2202), Independent Commission Against Corruption, New South Wales*

22. *Best Practice in Fraud prevention – Russell G Smith. Australian Institute of criminology – trends & issues in crime and criminal justice*

23. *Managing the Risk of Fraud: The ALARM Standard for Risk Advisors. ALARM – The National Forum for Risk Management in Public Sector*

24. *Fraud and Corruption Detection System (a presentation) by World Bank and Ministry of Health, GoI.*

25. *A Survey into Fraud Risk Mitigation in 13 European Countries – Ernst& Young*

26. *Value of Internal Audit in Fraud Detection (May 2006) – Paul Coram, Colin Ferguson and Robyn Moroney, Department of Accounting and Business Information Systems, Australia*

27. *Statistical Fraud Detection: A Review by Richard J Bolton and David j Hand, Statistical Science, 2002, Vol.17. No.235-255*

28. *Strategic Fraud Detection: A Technology-based Model – Conan C Albrecht and W Steve Albrecht, Rollins Centre for eBusiness*

29. *Strategic Control Plan in Dealing with Fraud and Corruption by Peter John Lynch of Lynch Investigation & Countermeasures Pty Ltd.*

30. *The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data, Cindy Durtschi, William Hillison and Carl Pacini, Journal of Forensic Accounting 1524-5586/Vol V(2004)*

31. *Fraud Act 2006 – United Kingdom*

32. *Law Commission of India – Twenty Ninth Report on Proposal to include certain social and economic offences in the Indian Penal Code, Government of India (1966)*

33. *Law Commission of India – Forty-Seventh Report on the Trial and Punishment of Social and economic Offences, Government of India (1972)*

34. *Law Commission of India – One Hundred Fifty-Sixth Report on the Indian Penal Code, Government of India (1977)*

35. *The Report of the RBI Expert Committee on Legal Aspects of Bank Frauds-2001*

36. *LATVIA - Report on Anti-Fraud System – 2001; SIGMA; 2001*

37. *Cyber Law & Information Technology - Talwant Singh*

38. *Fighting Corruption - What Role for Civil Society? The Experience of the OECD*

39. *State of Fraud and Corruption;* Asian Organization of Supreme Audit Institutions (*ASOSAI)*

40. *The Precarious State of Public Finance, 2007 - Jens Martens;*

41. *Shadow Economics of 145 Countries all over the World: Estimation Results over the Period 1999 to 2003; 2005 - Friedrich Schneider*

42. *Legislative Measures to Deal with Economic Crimes in India - Animesh Bharti*

43. *Fraud and white-collar crime: Power Against corruption; 2008 - Stephen Gentle*

44. *Fraud and white-collar crime: Tough tackle; 2008 - Andrew Horrocks and Sarah Crowther*

45. *Conference on Combating Corruption in Asian and Pacific Economies; Asian Development Bank*

    http://www.adb.org/documents/speeches/1999/ms1999012.asp

46. *Defining Corruption - Glossary of International Standards for Criminalization of Corruption; OECD Observer*

47. *Action Plan Implementation Projects 2002-03; ADB OECD Anti-Corruption Initiative for Asia-Pacific*

48. *Anti-Corruption Action Plan for Asia and the Pacific*

    http://www1.oecd.org/daf/ASIAcom/ActionPlan.htm

49. *The World Bank's Approach to Combating Corruption 2006 - Vinay Bhargava, Director, Operations & International Affairs*

50. *Anti-Corruption Action Plan for Asia and the Pacific, 2005 - Asian Development Bank;*

51. *The Fight Against Fraud - OLAF*

52. *What is Corruption - OECD Observer*
    http://www.oecdobserver.org/news/fullstory.php/aid/233

53. *Black Money: Big, Black & Booming - Anjuli Bhargava & Jehangir S. Pocha*

54. *Fraud Control - A State Perspective; 2000 - Brendan Bulter SC, Criminal Justice Commission, Qld.*

55. *Dirty Money and its Global Effects; - Published in International Policy Report; 2003 - Raymond Baker, Brionne Dawson, Ilya Shulman & Clint Brewer*