भारतीय मानक

संस्था द्वारा जालसाजी और भ्रष्टाचार नियंत्रण संबंधित मार्गदर्शिका

Indian Standard

GUIDANCE ON FRAUD AND CORRUPTION CONTROL BY AN ORGANIZATION

ICS 03.100.01

B U R E A U   O F   I N D I A N   S T A N D A R D S
M A N A K   B H A V A N ,   9   B A H A D U R   S H A H   Z A F A R   M A R G
NEW DELHI 110002

May 2010   **Price Group 7**

Social Responsibility Sectional Committee, MSD 10

FOREWORD

This Indian Standard was adopted by the Bureau of Indian Standards, after the draft finalized by the Social Responsibility Sectional Committee had been approved by the Management and Systems Division Council.

The awareness of risks and consequences of fraud and corruption has been increasing across the organizations in recent years. Reports by various audit and accounts institutions and committees have all highlighted the impact that fraud and corruption can have on the productivity, image and efficiency of an organization and on all aspects of organizational administration. Bribery and corruption of all kinds undermines trust, inhibits social and economic development and undermines fair competition.

There are several reasons why the elimination of corruption is becoming a high priority within the business community as well. Confidence and trust in business among investors, customers, employees, and the public generally has been eroded by a wave of business ethics scandals in recent years. Further, several high profile cases of bribery are currently being investigated or prosecuted.

Organizations are learning the hard way as to how they can legally and socially be held responsible for the deeds and misdeeds of their staff due to ineffective or non-existing controls for checking the activities of their staff. In recent years, it is seen that many corporates have even collapsed due to incidences of fraud and corruption involving financial statements, excessive payment of remuneration, etc, due to which many people had lost their savings and even livelihood, eroding the credibility and image of the organization.

Examples of common fraud could include theft of plant, equipment and inventory by employees; False invoicing; Theft of funds; Lending fraud; Misappropriation of remittance received by an organization; Credit Card fraud; Theft of intellectual property; Falsification of financial accounts of the organization for undue benefits; Theft of confidential organization information for private gains; Tax evasion; Money laundering, etc. There could be varied reasons for the increasing number of fraud which would depend on varying factors including type and nature of activities of the organization; its functioning; use and reliance on technology; rapid and continuous changes to business operations, etc, without appropriate safeguards.

All organizations should, therefore, make every effort to ensure that the control systems in place are sound and are designed with a view to prevent fraud and corruption, which could include financial regulations, anti-fraud policies, provision of trained fraud investigators, fraud awareness training for all staff, codes of conduct, etc. However, the threat of control weakness and fraudulent or corrupt activities always remains.

To ensure that all weaknesses in internal control and allegations of fraud or corruption, whether actual or perceived, are adequately reported by the staff by using the established procedures or other appropriate action, the organization should devise ways and means of checking it.

The composition of the Committee responsible for the formation of this standard is given at Annex D.

Indian Standard

GUIDANCE ON FRAUD AND CORRUPTION CONTROL BY AN ORGANIZATION

1 SCOPE

1.1 This standard provides guidance for prevention and control of fraud and corruption by an organization irrespective of its size, type, location or nature of activities.

1.2 This standard is generic and is not intended to enforce uniformity of practices or overwrite the existing rules and regulations as they would vary from organization to organization depending upon its structure, policies, objectives, products and services, processes and specific practices employed.

2 TERMS AND DEFINITIONS

For the purpose of the standard, the following terms and definitions should apply. The definitions and text given in legal, statutory and regulatory requirements may be referred for legal connotation.

2.1 Bribe — Monetary or other favour given or promised in order to induce or influence the judgment or conduct of a person in a position of trust.

An act of bribe means and includes, taking or giving any valuable or pecuniary benefit, not due, or causing favour or disfavour as an inducement or reward for doing or forbearing to do an act relating to exercise or non-exercise of power in office in the course of official duty with malafide intention.

2.2 Corruption — Dishonest activity in which the management, employee or any person acting on behalf of or dealing with an organization acts contrary to the interests of that organization and/or abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself or for another person or organization.

NOTE — An activity of corruption may include accepting or obtaining or agreeing to accept or attempting to obtain; giving or agreeing to give or offering any undue gratification or causing favour or disfavour to any person or entity as an inducement or reward for doing or forbearing to do an act relating to the exercise or non-exercise of power in office in the course of official duty with malafide intention.

'Malafide intention' includes any action motivated by or resulting, *inter alia*, in any one or more of the following:

    a)   Dishonest act;

    b)   Abuse of authority;

    c)   Use of position of trust for dishonest gain;

    d)   Giving or enabling a person to receive preferential treatment; or

    e)   Abuse of public resources.

2.3 Evidence — It is generally referred to as anything that is used to determine or demonstrate the truth of an assertion.

NOTES

1 Evidence is any species of proof on probative matter used to determine or demonstrate the truth of an assertion. It means and includes oral testimony in relation to matter(s) in issue, documents including electronic records and their analysis, material exhibits and facts deduced from circumstances on the basis of objective criteria.

2 Evidences could be presented during departmental inquiry, legal proceedings, Court trials, investigations, etc.

2.4 Fact, means and includes,

    a)   anything, state of things, or relating to things, capable of being perceived by the senses; and

    b)   any mental condition of which any person is conscious.

2.5 Fraud — Dishonest and/or deceptive activity, causing actual or potential loss to any person or organization.

NOTE — This may include theft of money or other property by employees or persons external to the organization. This also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position.

2.6 Fraud and Corruption Control Plan — A document summarizing an organization's anti-fraud and anti-corruption strategies.

2.7 Fraud and Corruption Risk Assessment — The application of its management principles and techniques in the assessment of the risk of fraud and corruption within an organization.

2.8 Risk — The chance of something happening that will have an impact upon achievement of the objectives of the organization.

2.9 Residual Risk — The remaining level of risk, after risk treatment measures have been taken.

2.10 Effective (in the Context of Internal Control Effectiveness) — An internal control which, though not providing a total solution to a particular fraud or corruption risk, if operated as intended, will make a positive contribution to mitigating the risk of fraud and corruption under consideration.

2.11 Ineffective (in the Context of Internal Control Effectiveness) — An internal control which, by reason of its not operating as intended or some other factor, is making no contribution to mitigating the risk under consideration.

2.12 Partially Effective (in the Context of Internal Control Effectiveness) — An internal control which, by reason of its not operating as intended or some other factor, is making some contribution to mitigating the risk under consideration.

2.13 Investigation — Investigation means and includes ascertainment of truth on the basis of oral testimony, document(s) and its analysis, material exhibits and facts deduced from circumstances on the basis of objective criteria by any person on being entrusted by competent authority.

It would also include linking any person (either a natural person or a body corporate) with conduct that violates any law or the policies and standards set by the concerned organization.

2.14 Secret Commission — A payment in money or in kind which will or is intended to cause a person to act in a way that is contrary to the interests of his or her principal or employer or is contrary to the principal or employer's policy on a given issue or is against the public interest. Secret commissions, by definition, will typically be paid without the knowledge or express or implicit agreement of the principal and include payments intended to influence the outcome of specific action or event as well as the actions generally over a period of time.

2.15 Top Management — Person or group of people, who directs and controls an organization at the highest level.

> NOTE — Typically top management is the highest authority that is empowered to take all decisions on policy, resources and external matters in relation to the organization.

3 DOCUMENTATION

3.1 General

An effective system for fraud and corruption control would entail the establishment of documents describing the processes for planning and monitoring of the control measures and the results of these processes. Such documentation may include,

a) a manual for fraud and corruption control;

b) procedures for planning and monitoring of control processes;

c) procedure for receiving and handling information relating to fraudulent and corrupt activities;

d) procedures for conducting investigations and enquiries;

e) a classification of activities that are considered to be fraudulent and/or corrupt and the penal actions that may be taken against delinquent employees;

f) instructions issued to work force describing the desired rules of conduct and preventive measures;

g) documents of external origin that may apply to the organization and to its employees;

h) any other document needed by the organization for effective planning, operation and control; and

j) records required by this standard.

The extent of documentation would differ from one organization to another due to the nature and complexity of processes and their interactions, size of the organization and the perceived risks encountered.

3.2 Fraud and Corruption Control Manual

A typical manual may include the following:

a) Organization's anti-fraud and anti-corruption policy;

b) Organization's objectives for effective control of fraud and corruption;

c) The risks identified with respect to fraud and corruption;

d) Risk management system for dealing with the identified risks;

e) The organizational structure for dealing with fraud and corruption control including responsibility and authority of personnel at relevant levels for,

   1) taking preventive actions;

   2) initiating and taking investigative actions on detection of actual or potential incidences of fraud and/or corruption;

   3) initiating and taking punitive/corrective actions following establishment of fraudulent and/or corrupt practice; and

   4) liaisoning with law enforcement agencies where their intervention becomes necessary.

f) Other documents described at **3.1** (b) to (h) or a reference to them.

3.3 Control of Documents

The various documents established by the organization should be approved for adequacy, completeness and accuracy and should also be reviewed periodically for updation. The control should ensure that obsolete documents are removed to avoid their unintended use. Documents should be legible and easily identifiable indicating their current revision status. It is always a good practice to maintain a master list and a distribution list of all such documents so that the current version of the applicable/revised documents could be made available to all concerned. This would facilitate effective communication of all new procedures and policies laid down by the organization for fraud and corruption control.

3.4 Control of Records

The organization should establish and maintain relevant records for effective control and implementation of the fraud and corruption policies and objectives. They should be legible, easily identifiable and easily retrievable. The organization should establish the method of identification, storage, protection, disposition of each record, their retention time and responsibility for each of these activities. The safeguards to prevent unauthorized access to records may also be established and maintained.

4 MANAGEMENT RESPONSIBILITY

4.1 Management Commitment

Top management should,

a) establish anti-fraud and anti-corruption policy and strategy;

b) ensure that fraud and corruption control objectives are established;

c) ensure voluntary compliance with internal codes of organization's principles and ethics and with external/universal guidelines;

d) set up and reinforce high standards of behaviour as the norm while identifying, reducing and rectifying incidences of non-compliance;

e) not send misleading signals and behave in unethical manner while laying down or adopting organization's policies and practices;

f) ensure that an ethical culture is developed within the organization;

g) make continuous efforts to ensure that fraud and corruption principles and codes are integrated with the various management systems of the organization;

h) conduct management reviews;

j) ensure availability of resources;

k) be accountable and transparent; and

m) create an atmosphere conducive to encouraging employees to report weakness(es) in the system for plugging loopholes as also prevent incidences of fraud and corruption.

4.1.1 The top management should ensure that the policies and procedures established for fraud and corruption control are communicated and made available to all personnel and also understood within the organization.

4.2 Objectives

4.2.1 The organization should lay down fraud and corruption control objectives, which should be consistent with the anti-fraud and corruption policy. These objectives could be,

a) elimination of internally and externally instigated fraud and corruption against the organization;

b) formulation of appropriate working procedures for various functionary segments to prevent internal frauds and pinpoint aberrations by delinquents;

c) initiation of appropriate remedial action for modification of working procedures and against delinquents in case of failure to prevent fraud and corruption;

d) detection of all instances of fraud and corruption against the organization in the event that preventative strategies fail;

e) recovery for the organization of all property dishonestly appropriated or secure compensation equivalent to any loss suffered as a result of fraudulent and corrupt conduct; and

f) suppression of fraud and corruption by organizations against other organizations.

4.2.2 Department-wise measurable objectives could also be laid down at relevant functions and levels.

4.2.3 However, while establishing the above policies and objectives, the organization should take into account the inputs and feedback from employees and other stakeholders including relevant legal, statutory and regulatory requirements as also other universal guidelines/conventions, if any. These could also be based on the feedback received or outcome of the analysis made by the risk management team.

4.3 Responsibility, Authority and Communication

4.3.1 Top management should ensure that the

responsibilities and authorities are established at relevant functions and levels and are communicated within the organization.

4.3.2 A committee comprising senior management should be established for controlling the risks of fraud and corruption within the organization and by other organization, that is, in terms of the organization's dealing with other parties. The members of the group should be selected judiciously keeping in view their unblemished track record, ethical behaviour, a high degree of consciousness and awareness about the risks of fraud and corruption as also the activities and objectives of the organization. They should be imparted suitable training in this regard including awareness of new types of technology that is being used for the commission of fraud and also the technological measures that can be used by an organization to minimize these new types of fraud, for example, cyber frauds.

4.3.3 This Committee will be responsible to implement the organization's fraud and corruption control strategies. They may take the assistance of specialized personnel, if required. The Committee should be accountable to ensure compliance to the various provisions, as contained in this standard. It should also be responsible to coordinate the fraud and corruption risk assessment process, to record and collate fraud and corruption incident reports and to conduct or coordinate the organization's investigations into allegations of fraud and corruption. The management should delegate commensurate authority for effective discharge of their duties and responsibilities. Refer also to flow chart given at Annex B for typical responsibilities of compliance.

4.3.4 The top management should designate an employee, preferably from senior management, as a compliance officer, who irrespective of other responsibilities, would,

a) carry out the fraud and corruption control functions including formulation of fraud and corruption control systems, in consultation with other management, staff and external agencies;

b) be responsible for receiving and handling information as well as coordinating activities relating to fraud and corruption in the organization;

c) liaison with law enforcement agencies, whenever needed;

d) report to the top management regarding the performance of fraud and corruption control functions and systems in the organizations;

e) coordinate management review meetings;

f) coordinate internal audits and report significant findings to the top management;

g) report to the top management regarding significant feedback including complaints/ information received relating to fraud and corruption; and

h) act as the Member Secretary of the Committee, mentioned at **4.3.2**.

4.3.5 *Internal Communication*

Top management should ensure that appropriate communication processes are established within the organization so that effective communication takes place at all levels for the various processes related to fraud and corruption control.

4.4 Fraud and Corruption Control Planning

4.4.1 Organizations should develop and implement an appropriate fraud and corruption control plan. This plan should be periodically reviewed and modified as required. Organizations operating in rapidly changing technological environment may need to review the plan more frequently. Responsibilities and authorities for the implementation and on-going monitoring of the plan should be defined keeping in view the competency and experience of the personnel, organizational and financial infrastructure of the organization. Adequate time should be given to the personnel for discharge of their responsibilities.

4.4.2 The organization's commitment to and implementation of the fraud and corruption control plan should be well publicized to all stakeholders. The management and staff should regularly be communicated about the fraud and corruption control issues including modifications made therein from time to time and current best practices.

4.4.3 A strategy or procedure for monitoring the implementation of the fraud and corruption control plan, specifying both internal and external monitoring processes, should be established outlining the schedule of the control programme, resources needed and the data to be collected for effective control and analysis. This strategy should periodically be reviewed for continued suitability, effectiveness and improvements.

A typical fraud and corruption control plan is given in Annex A.

4.5 Management Review

4.5.1 Top management should review the organization's management system for fraud and corruption control procedures and policies at planned intervals to ensure their continuing suitability, adequacy, efficiency and effectiveness. This review

should include assessing opportunities for improvement and the need for changes in various policies and procedures, based on the experience gained, technological developments and feedback received. The records of management reviews should be maintained.

4.5.2 The inputs to management review should generally include information on,

a) follow up actions from previous reviews;

b) results of audit;

c) feedback received including both internal and external sources;

d) effectiveness of control measures;

e) review of process performance of fraud and corruption control measures;

f) benchmarking results *vis-à-vis* other similar organizations;

g) technological changes; and

h) recommendations for improvement.

4.5.3 Review output should include any decisions and actions related to,

a) improvements in fraud and corruption strategies/procedures/control plans;

b) improvement in ethical culture of the organization;

c) improvement in management systems needed for fraud and corruption control; and

d) resources needed.

5 RESOURCE MANAGEMENT

5.1 The organization should determine and provide resources for effective implementation of management systems for fraud and corruption control. The resources should include human resources, infrastructure and work environment. This would include allocation of specialized personnel on full time or part time basis to implement the organization's fraud and corruption control strategies, to coordinate the fraud and corruption risk assessment process, to record and collate fraud and corruption incident reports and to conduct or coordinate the organization's investigations into allegations of fraud and corruption. Allocation of adequate resources would also include engagement of specialist resources (internal or external to an organization) with the requisite skills and experience, in case needed.

5.2 The organization should aim to ensure that it has a healthy and sustainable ethical culture through a process of benchmarking and continuous monitoring. If it falls below the desirable limit then remedial action including a broad based communication and training program should be undertaken.

5.3 Experience has shown that one of the most common and effective ways in which fraud and corruption is detected is by observation, investigation and reporting by fellow workers of the perpetrator(s). It is, therefore, vital that every staff member has a general awareness of fraud and corruption and how he/she should respond if this type of activity is detected or suspected. Organizations should regularly communicate to staff a clear definition of the types of action that constitute fraudulent or corrupt practice, the fraud detection measures that are in place and an unequivocal statement that fraudulent and corrupt practices within the organization will not be tolerated.

5.4 The organization should, therefore, ensure that the personnel are,

a) selected on the basis of capability to satisfy defined job specification. Intrinsic motivation for this type of responsibility should be an important criteria;

b) trained to ensure that they understand the tasks to be performed and the objectives to be achieved, and they personally identify with the whole process;

c) trained in code of conduct at induction and throughout the period of their training;

d) aware of fraud and corruption and how he/she should respond if this type of activity is detected or suspected;

e) fully aware of the controls that are in place in their organization;

f) complying with such control procedures at all times;

g) understand the importance of adhering to the controls at all times;

h) made aware about the modification made in the procedures and policies from time-to-time through training, newsletters or other internal communications;

j) taking all reasonable steps to ensure that controls are complied with by others. This is particularly relevant for supervisory or managerial staff;

k) sensitized to report potential control weaknesses to the appropriate authority; and

m) made aware of the past significant cases of fraud and corruption and corrective/preventive actions taken thereof.

5.4.1 The training records should be maintained.

5.5 Infrastructure and Work Environment

The organization should determine, provide and maintain the infrastructure and work environment necessary for achieving the objectives of effective fraud

and corruption control. Work environment conducive to promoting equity, fairness and transparency need to be maintained.

6 FRAUD RISK MANAGEMENT

6.1 Fraud risk management involves establishing an appropriate infrastructure and culture and applying a logical and systematic method of establishing the context, carrying out identification, analysis, evaluation, treatment, and monitoring of risk, and carrying out communication on risks associated with any activity, function or process in a way that will enable an organization to minimize adverse impacts. The risk management policy should be fully integrated into the general policy of the organization and specific objectives and criteria of a particular project or activity should be considered in the light of objectives of the organization as a whole.

6.2 Establishing the context defines the basic parameters within which risks must be managed and sets the scope for the rest of the risk management process. The context may include financial, operational, political (public perceptions and image), social, environmental, cultural, legal and other aspects.

Management of risk should not be a 'stand-alone' activity or be separate from the main activities and processes of the organization but should be part of the accountabilities responsibilities of line management and an integral part of the normal organizational processes as well as of all project and change management processes.

6.3 Before starting to develop a risk management plan, the organization should critically review and assess those elements of the risk management process that are already in place. This review should reflect the risk management needs of the organization and its context. The review should deliver a structured appreciation of,

    a) the maturity, characteristics and effectiveness of existing organizational function and risk management culture and systems;
    b) the degree of integration and consistency of risk management across the organization and across different types of risks;
    c) the processes and systems that should be modified or extended;
    d) constraints that might limit the introduction of more systematic risk management;
    e) legislative or compliance requirements; and
    f) resource constraints.

6.4 Once the context is established, the risks emanating or associated with the organization's activities and its stakeholders should be identified, analyzed, evaluated

and treated to minimize or mitigate their impact on organization's activities, processes, image, ethical culture, etc. The various steps involved in any Fraud Risk Management are:

    a) *Risk identification* — The process of recognizing and recording risks can include determining who, why, what, when, where and how.
    b) *Risk analysis* — The process of systematic use of information to estimate/understand the risk which may provide a basis for *risk evaluation* and *risk treatment*. The information can include historical data, theoretical analysis, informed opinions, and the views of interested parties.
    c) *Risk evaluation* — The process of comparing the results of the *risk analysis* against given risk criteria to determine the significance of the risk. It assists in making the decision about *risk treatment*.
    d) *Risk treatment* — The process of selection and implementation of measures to modify risk. This may also include management controls.

    NOTE — The term 'risk treatment' is sometimes used for the measures themselves.

    e) *Risk assessment* — The overall process of *risk identification*, *risk analysis* and *risk evaluation*.

A typical fraud and corruption control plan is given in Annex A.

6.5 The organization should establish a procedure for fraud and corruption control process which could include the following:

    a) Identification of fraud and corruption prone areas in a systematic manner;
    b) Identify potential consequences of a failure or weakness in control procedures and take all reasonable steps to ensure that such control procedures are sufficiently robust to prevent fraud and corruption;
    c) In case during the normal activities, control weaknesses are identified, whether actual or perceived, the same should be reported, including potential consequences, to the top management or any other person responsible for the same;
    d) Documentation of the process of risk identification; and
    e) The record of the risk identified and prescribed treatment plan should be retained for future reference.

6.5.1 The output of this procedure should be in the

form of identified risks, duly prioritized and the prescribed treatment for these.

6.6 An internal reporting system may include the following:

a) *Communication* — Making various provisions of the above procedures known to all employees.

b) *Accessibility* — Making the control programme available throughout the organization.

c) *Cultural Appropriateness* — Adapting the control programme to suit local cultures.

d) *Openness* — Making the reporting system also available to suppliers, consultants and customers.

e) *Screening* — Provide safeguards against frivolous or malicious reports.

f) *Collect Data* — Monitor reports, track them over time and identify weaknesses.

g) *Remedial Action and Feedback* — Take action and provide feedback.

h) *Management Visibility* — Report to the audit committee or any other appropriate authority.

j) *Employee Protection* — Protect reporting employees.

k) *Confidentiality* — Information/action to be kept confidential to avoid harassment to innocent persons while at the same time not letting the person involved cover up his/her tracks or fiddle with evidences.

m) *External Communications* — Report to stakeholders and other interested parties on actions taken and results achieved.

6.7 Procedure for Dealing with Suspected Fraud or Corruption

6.7.1 The organization should establish a documentary procedure for dealing with the detected and/or suspected incidences of fraud and corruption. The procedure may include some or all of the following steps depending upon the type and size of the organization:

6.7.1.1 *Preliminary examination*

The organization may conduct an examination to establish a *prima-facie* case for subsequent investigation.

6.7.1.2 *Investigation*

Investigation should be carried out by competent personnel, independent of the area where incidence of fraud and corruption has been established. The

organization should identify and establish appropriate methods for carrying out the investigation.

6.7.1.3 *Disciplinary proceedings*

The organization may conduct disciplinary proceedings in case it is decided to take disciplinary action against the employee(s) concerned. The disciplinary proceedings should be conducted by competent personnel, as designated by the management, independent of the area where incidence of fraud and corruption has been established. All the employees of the organization should be informed, through suitable means, about the procedure for disciplinary proceedings and the type, nature and consequences of the penalties likely to be imposed in case the charges framed against the employee(s) are held as 'proved' during the disciplinary proceedings, as also the redressal mechanism.

The disciplinary proceedings should be conducted in a fair and impartial manner, observing the principles of natural justice, by taking into account all facts and circumstances of the case.

6.7.1.4 *Prosecution*

The organization should frame an appropriate policy and identify suitable method(s) for reporting the detected incidences of fraud and corruption to the law enforcement agencies. This may also include provision of material evidence to support the law enforcement agencies in their further investigation.

6.7.1.5 *Recovery*

The organization may establish suitable policy and procedure for initiating recovery action in the cases of detected incidences of fraud and corruption.

6.8 Each incident of fraud and corruption should be evaluated for its impact on,

a) stakeholder;

b) organization's reputation;

c) finance; and

d) affected and allied processes.

6.8.1 The organization should have suitable plans to manage the incident which may include:

a) containing the effect of damage;

b) resumption of normal working;

c) recovery of financial losses through insurance; and

d) handling of communication to internal/external stakeholders and media.

6.8.2 A typical model for fraud and corruption risk management is given in Annex C.

7 IMPLEMENTATION, MONITORING, MEASUREMENT AND IMPROVEMENT

7.1 Implementation

7.1.1 The organization should,

a) introduce anti-fraud and anti-corruption policies and programmes within the organization;

b) identify and implement the applicable legal, statutory and regulatory requirements;

c) set up an effective risk assessment procedure entailing laying down processes aimed at identifying, assessing, prioritizing and eliminating all potential risks identified in an organization with action plan and consequences thereof;

d) make provisions for a formal feedback system once a year from the major stakeholders including employees of the organization and outside parties (affected directly or indirectly) dealing with the organization;

e) introduce some mechanism of recognizing personnel for providing information on fraud and corruption incidences;

f) adopt internal reporting procedures to ensure that appropriate systems and reporting mechanisms are in place that assures that the management is first to know about any malpractice, as and when it occurs;

g) report on the work against fraud and corruption in their annual reporting system;

h) share experiences and best practices with other interested organizations;

j) provide information on the recent legal development, voluntary initiatives, and emerging best practices in the areas of encouraging reporting, making disclosures and protecting staff who are prepared to speak up when malpractice occurs with the organization;

k) educate concerned stakeholders for prevention of incidences of fraud and corruption;

m) replacement/rotation of working personnel in prone area to avoid set corruption practices/fraud, wherever practicable;

n) widely publicize the contact details of the compliance officer;

p) provide protected boxes for reporting; and

q) set up a mechanism for receiving and handling information relating to fraudulent and corrupt activities including complaints handling.

7.1.2 One of the preventive strategies adopted by organizations dealing with large scale or repeated procurements is the execution of an 'Integrity Pact' with the suppliers/service providers, etc. The integrity pact, which is amalgamated into the tendering process,

a) seeks written assurance from all parties participating in the selection process for scrupulous adherence to free, fair and honest transactions at all stages;

b) encourages the development of Code of Conduct among bidding organizations;

c) provides for summary termination of contract for breach of terms and disqualification from participating in future procurement processes;

d) provides for regular monitoring by independent experts of the progress and compliance to terms of contract; and

e) includes a mechanism for arbitration in case of disputes.

7.1.3 It is generally observed that there is a strong link between the incidence of fraud and corruption within an organization and poor internal control systems. In many cases where fraud and corruption is detected, it is possible to identify a fundamental internal control weakness or failure that either allowed the incident to occur or failed to detect it quickly after it occurred. The organizations should, therefore, implement systems aimed at quickly identifying instances of fraud and corruption in the event that prevention strategies fail. These systems could include targeted post transactional review; strategic use of computer based reporting systems; analysis of management accounting reports, etc.

7.1.3.1 Organizations should install appropriate policies and procedures for dealing with suspected fraud and corruption detected through its detection systems or otherwise coming to their notice. This will include the development and implementation of,

a) protocols for reporting the matters of suspected fraud and corruption to the appropriate law enforcement agency;

b) appropriate measures for the comprehensive investigation of such matters based on the principles of independence, objectivity and the rules of natural justice;

c) policies for the recovery of the stolen funds and property; and

d) mechanism for determination of the extent of action against the delinquent person.

7.1.3.2 Organizations should ensure that adequate means for reporting suspicious or known illegal or unethical conduct are available to all personnel

including proper mechanism with provisions for anonymity and requisite safeguards for the person conveying information/observation/investigation/or reporting the possibility or the existence of fraud. This could include an appropriate system for reporting concerns through the organization's usual organizational structure.

However, at the same time, the top management should chalk out strategies to protect the employees/whistle blowers who are reporting incidences of fraud and corruption.

7.1.3.3 The organizations should ensure that the line managers and senior management are aware of their accountabilities for the prevention and detection of fraud and corruption. The management of fraud and corruption should be incorporated into the performance measurement system and each line manager's performance should be measured against appropriate industry benchmarks.

7.1.3.4 Organizations should conduct pre-employment screening of all new employees appropriate to their position description in order to gain a reasonable understanding of the candidate's employment history and make decision about his/her employment accordingly.

7.1.3.5 Organizations could consider taking up insurance cover against the risk of fraud, corruption and theft of the organization's property, as part of the organization's overall insurance programme and include a consideration of the level of cover, inclusions/exclusions and deductibles.

7.2 Monitoring and Measurement

The organization should,

a) conduct periodic reviews to assess the effectiveness of the actions;

b) carry out analysis of each action to ensure their effective implementation;

c) involve external experts in the review of fraud and corruption control strategies, for example, expertise in IT, legal, etc;

d) benchmark its performance in the above area against that of other organizations performing similar functions;

e) share information with interested organizations about fraud/corruption incidences;

f) compare the benefits flowing from each control action with the intended benefits and make necessary modifications, if needed;

g) receive feedback from monitoring;

h) evaluate effectiveness of control programme; and

j) evaluate the ethical culture of the organization.

7.3 Internal Audit

The organization should conduct internal audits at planned intervals, at least once a year, to determine the compliance of the management systems for fraud and corruption control and other documents established by the organization. It should address all organization's risks and be used effectively to assess the preparedness of the organization towards prevention and detection of fraud and corruption in the organization. It should also incorporate adherence to internal controls by the personnel.

An audit plan should be made indicating the scope, frequency of audit, auditor(s), auditee and audit date(s)/time. Auditors should be selected on the basis of their competence and ability to conduct audit in the respective area and maintain objectivity and impartiality of the audit process. In case the requisite competence is not available in-house, then the assistance of external expert may be taken. Auditors should not audit their own work. The auditee should ensure that actions are taken without undue delay to eliminate detected non-conformities, deficiencies and their causes. Follow up activities should include the verification of actions taken and reporting of verification results. Records of audits should be maintained.

7.4 Analysis of Data

The organization should analyze the data collected during monitoring and measurement and feedback received to determine current level of performance and opportunities for continual improvement, particularly in areas where the incidence of fraud and corruption are repeatedly reported. The data relating to past fraud and corruption cases and non-compliance to legal, statutory and regulatory requirements should also be analyzed.

7.5 Improvement

7.5.1 *Corrective and Preventive Actions*

7.5.1.1 The organization should develop a system for prevention and detection of the incidences of fraud and corruption before they actually occur. The organization should take action to eliminate the cause(s) and potential cause(s) of fraud and corruption in order to prevent recurrence and occurrence respectively. These should be appropriate to the extent and effects of the incident reported and potential problems. Records of action taken and improvements effected should be maintained. The internal controls should be periodically reviewed for continual improvement.

7.5.1.2 For incidences of detected fraud and corruption, the internal control procedures should be reviewed by the management for adequacy and effectiveness with a view to plug loop holes as also for identifying improvements. The modified internal control procedures should suitably be communicated to all concerned within the organization for implementation and compliance.

ANNEX A

(*Clauses* 4.4.3 *and* 6.4)

FRAUD AND CORRUPTION CONTROL PLAN

A-1 A typical fraud and corruption control plan may include:

a) identifying the fraud and corruption prone areas;

b) identification of the decision-making process that influences the interests of external parties;

c) determination of the risks for corruption in terms of severity of impact, likelihood and extent;

d) identification of the process where fraudulent practices could occur;

e) determination of the risks for fraud in terms of severity of impact, likelihood and extent through the FMEA mode;

f) enlisting the significant risks;

g) the control measures applied in respect of each process for eliminating and reducing risk;

h) typical actions may include introducing verification checks, broad-basing critical decision-making process; e-governance; public disclosure of standards of service, procedures, records and reports; an effective complaints and appeals procedure; security cameras; information security management system; deterrent actions; whistleblower schemes; 'value watch' schemes; reducing discretion, periodic job rotation/transfer in fraud and corruption sensitive area, involvement of stakeholders in complaints handling process, etc;

j) The records of control measures, non-conformances observed and cases of fraud and corruption detected; and

k) The persons responsible for these actions;

m) Recognition scheme.

NOTE — Whistle blower scheme are the common methodology used by organizations for protecting the identity of the person reporting the incident of fraudulent and corrupt practices in the organization.

ANNEX B

(*Clause* 4.3.3)

PROCESS FLOW CHART

```
┌─────────────────────────────────────────────────┐
│  Establish anti-fraud and anti-corruption policy │
└─────────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────────┐
│     Establish anti-fraud and anti-corruption     │
│                   objectives                     │
└─────────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────────┐
│      Establish codes of ethics and conduct       │
└─────────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────────┐
│     Identify fraud and corruption prone areas    │
└─────────────────────────────────────────────────┘
          │                           │
          ▼                           ▼
┌────────────────────┐      ┌────────────────────┐
│  Identify decision-│      │  Identify fraud    │
│  making processes  │      │  prone sources     │
│  that influence    │      │  and processes     │
│  external party    │      │                    │
│  interest          │      │                    │
└────────────────────┘      └────────────────────┘
          │                           │
          ▼                           ▼
┌────────────────────┐      ┌────────────────────┐
│ Analyze risk for   │      │ Analyze risk for   │
│ corruption in      │      │ fraud in terms of  │
│ terms of impact,   │      │ impact, likelihood │
│ likelihood and     │      │ and extent for     │
│ extent for each    │      │ each identified    │
│ identified process │      │ process            │
└────────────────────┘      └────────────────────┘
          │                           │
          ▼                           ▼
┌─────────────────────────────────────────────────┐
│   Evaluate and enlist significant risks (with    │
│          respect to risk tolerance)              │
└─────────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────────┐
│            Risk treatment planning               │
└─────────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────────┐
│                 Risk treatment                   │
└─────────────────────────────────────────────────┘
                      │
                      ▼
┌─────────────────────────────────────────────────┐
│  Evaluate residual risk against risk tolerance   │
└─────────────────────────────────────────────────┘
                      │
                      ▼
                 ◇ Acceptable ◇
            No   ◇    risk    ◇
                 ◇           ◇
                      │
                     Yes
                      │
                      ▼
```
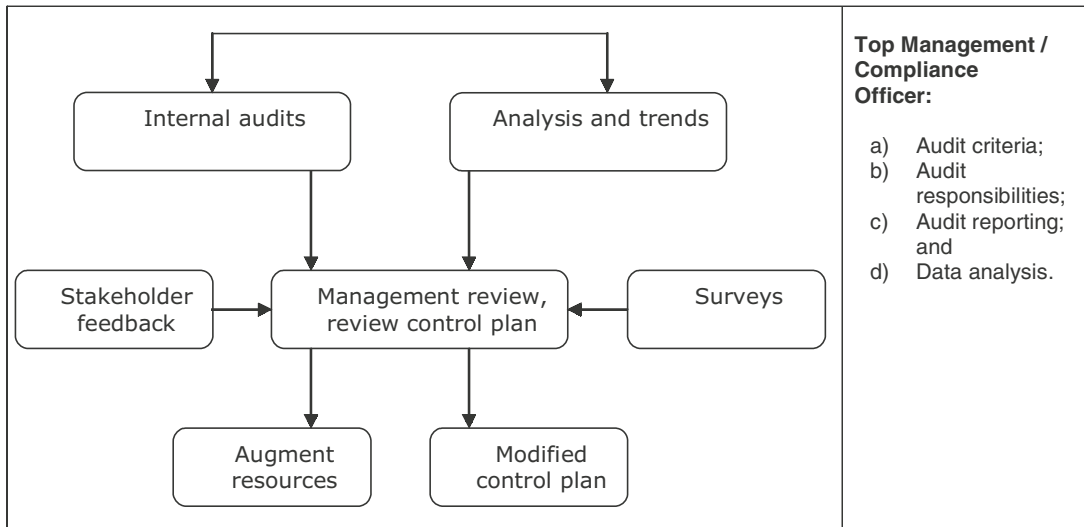
Top Management Processes

Compliance Officer: Consultation with internal / external stakeholders

Compliance Officer: Risk assessment through FMEA methodology

Risk level = Impact × Extent × Probability

Operational Processes
Manual,
Procedures,
Risk control plan:
- Responsibilities
- Deterrent and preventive steps
- Monitoring
- Verifications and checks
- Reporting routes
- Education and training
- Recording

Top Management / Compliance Officer:

a) Audit criteria;
b) Audit responsibilities;
c) Audit reporting; and
d) Data analysis.

ANNEX C

(*Clause* 6.8.2)

MODEL FOR FRAUD AND CORRUPTION RISK MANAGEMENT

A. Planning for Fraud and Corruption Risk Management	B. Fraud Prevention	C. Fraud Detection and Resolution

Scope of Fraud and Corruption Risk Management	Key Activities

B. Fraud Prevention

- Internal Controls
- Ethics Management

Internal Controls
- Sensitization and awareness
- Risk control measures
- Internal audits and review
- Information management

Ethics Management

Develop Code of Conduct
- Develop/review the code of conduct and other related policies to assess sufficiency, adequacy and clarity in terms of fraud and misconduct related issues

Role Out Effectiveness
- Developing recommendations that can be included in subsequent roll outs, revisions and refresher courses to make the process more robust and encourage use of these mechanisms by employees

C. Fraud Detection and Resolution

- Formal Process on Investigation
- Consequence Management

Investigation Process
- Selecting investigation team
- Collecting evidence
- Protecting interests
- Reporting

Consequence Management
- Clear communication on actions that can be taken
- Prosecution
- Recovery action
- Review/strengthening of internal controls

Fraud Response Plan
- Damage containment
- Recovery through insurance
- Resumption of normal working
- Stakeholder management
- Media management
- Internal and external communication

ANNEX D

(*Foreword*)

COMMITTEE COMPOSITION

Social Responsibility Sectional Committee, MSD 10

Organizations	*Representative(s)*
Department of Consumer Affairs, Ministry of Consumer Affairs, Food and Public Distribution, New Delhi	SHRI SANJAY SINGH (***Chairman***)
All India Carpet Manufacturers Association, District Varanasi, U.P.	SHRI SHAUKAT ALI ANSARI SHRI AVINASH CHANDRA BARANWAL (*Alternate* I) PROF (DR) KRISHNAKANT GOSWAMI (*Alternate* II)
Bharat Heavy Electricals Limited, New Delhi	SHRIMATI SUGUNA SWAMINATHAN
Cement Manufacturers Association, Noida	SHRI S. K. DALMIA
Confederation of Indian Industry, Gurgaon	SHRI ANANT G. NADKARNI SHRI SHIKHAR JAIN (*Alternate*)
Consumer Coordination Council, Noida	SHRI BEJON MISRA SHRI ARUN KUMAR (*Alternate*)
Consumer Education & Research Society, Ahmedabad	DR MALAY R. DAVE SHRI RAJAN R. GANDHI (*Alternate*)
Consumer Unity & Trust Society, New Delhi	THE DIRECTOR, DELHI RESOURCE CENTRE
Delhi Fire Service Headquarters, New Delhi	SHRI R. C. SHARMA SHRI A. K. SHARMA (*Alternate*)
Development Alternatives, New Delhi	DR (MS) K. VIJAYA LAKSHMI MS INDRANI MAHAPATRA (*Alternate*)
Faculty of Management Studies, University of Delhi, Delhi	PROF V. K. BHALLA
FICCI, New Delhi	MS RANU KULSHRESTHA
Goa Institute of Management, Goa	DR DIVYA SINGHAL
Indian Business Academy, Greater Noida	DR (MS) DIVYA KIRTI GUPTA
ITC Limited, Kolkata	SHRI ASHESH AMBASTA
Kamala Nehru College, New Delhi	DR (MS) SAVITA HANSPAL
M/s Accessability, New Delhi	SHRI VIKAS SHARMA
Ministry of Commerce & Industry, Department of Industrial Policy and Promotion, New Delhi	SHRI ZAKARIA KHAN YUSUFZAI
Ministry of Labour, New Delhi	SHRI S. K. VERMA
Ministry of Social Justice & Empowerment, New Delhi	SHRI V. B. PACHNANDA
Ministry of Textiles, New Delhi	SHRI JAMINI KUMAR SHARMA SHRI J. N. SINGH (*Alternate*)
National Safety Council, Navi Mumbai	SHRI K. C. GUPTA SHRI M. M. KULKARNI (*Alternate*)
NTPC Limited, New Delhi	SHRI DINESH AGRAWAL SHRI ASHOK CHAKRAVORTY (*Alternate*)
Office of the Development Commissioner Small Scale Industries, Ministry of Small and Medium Enterprises, New Delhi	SHRI V. S. KARUNAKARAN SHRI J. K. ARYA (*Alternate*)
Partners-in-Change, New Delhi	SHRI VIRAF MEHTA
Safety Action Group, Gurgaon	SHRI RAJAN R. GANDHI
Steel Authority of India, New Delhi	SHRI RAM MOHAN
Tata Motors Limited, Mumbai	SHRI M. B. PARALKAR SHRI D. M. DESHPANDE (*Alternate*)
The Society for Upliftment of Masses, New Delhi	SHRI J. BHUSHAN MS KAMAL SHARMA (*Alternate*)
Transparency International India, New Delhi	COL K. R. DHARMADHIKARY DR S. K. AGARWAL (*Alternate*)

Organizations	*Representative(s)*
Voluntary organization in the interest of Consumer Education, New Delhi	DR SRI RAM KHANNA DR (MS) SAROJINI SINGHAL (*Alternate*)
Directorate General, BIS	SHRI P. BHATNAGAR Scientist E and Head (MSD) [Representing Director General (*Ex-officio*)]

Member Secretary
SHRIMATI RENU GUPTA
Scientist 'D' (MSD), BIS

Panel on Fraud and Corruption Control, MSD 10/P-2

Ex-Chief Vigilance Officer, Bureau of Indian Standards, New Delhi	SHRI A. K. DHUL (***Convener***)
Additional Commissioner of Police, Mumbai	SHRI K. L. BISHNOI
Additional CVO, BHEL, New Delhi	SHRI HARSH KAYASTHA
Additional Deputy Commissioner of Police, Economic Offences Wing, New Delhi	SHRI K. K. VYAS
Central Bureau of Investigation, Kolkatta	SHRI H. C. SINGH
Central Bureau of Investigation Academy, Ghaziabad	SHRI V. P. ARYA
CII-ITC Centre of Excellence for Sustainable Development, New Delhi	SHRI SHIKHAR JAIN SHRI ANUPAM KAUL (*Alternate*)
Department of Management Studies, IIT Delhi, New Delhi	DR KANIKA T. BHAL
FICCI Socio-Economic Development Foundation, New Delhi	DIRECTOR
ICAI, New Delhi	CA. VINOD JAIN, FCA
KPMG, Gurgaon	SHRI DEEPANKAR SANWALKA SHRI RAHUL LALIT (*Alternate*)
Management Development Institute, Gurgaon	DR TANUJA SHARMA
Securities and Exchange Board of India, Mumbai	SHRI S. RAMANN
Serious Fraud Investigation Office, Ministry of Company Affairs, New Delhi	SHRI D. BHARDWAJ
Telecom Regulatory Authority of India, New Delhi	SHRI M. C. CHAUBE
Transparency International India, New Delhi	COL K. R. DHARMADHIKARY DR S. K. AGARWAL (*Alternate* I) SHRI P. S. PAWA (*Alternate* II)
V.V. Giri National Labour Institute, Noida	DR (SHRIMATI) POONAM S. CHAUHAN

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards : Monthly Additions'.

This Indian Standard has been developed from Doc No.: MSD 10 (334).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110 002
Telephones : 2323 0131, 2323 3375, 2323 9402   *Website*: www.bis.org.in

Regional Offices:			*Telephones*
Central	:	Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110002	2323 7617 2323 3841
Eastern	:	1/14 C.I.T. Scheme VII M, V. I. P. Road, Kankurgachi KOLKATA 700054	2337 8499, 2337 8561 2337 8626, 2337 9120
Northern	:	SCO 335-336, Sector 34-A, CHANDIGARH 160022	60 3843 60 9285
Southern	:	C.I.T. Campus, IV Cross Road, CHENNAI 600113	2254 1216, 2254 1442 2254 2519, 2254 2315
Western	:	Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400093	2832 9295, 2832 7858 2832 7891, 2832 7892

Branches: AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAJKOT. THIRUVANANTHAPURAM. VISAKHAPATNAM.

Laser Typeset by Sunshine Graphics