AUTHUM

RISK MANAGEMENT POLICY

Table of Contents

1. Overview

Company operates in dynamic environment & given the markets, growth & structure, elements of risk are inherent. The Board of the Company recognizes the importance of identifying and controlling risks and ensuring that required internal controls and procedures have been established which are designed to safeguard assets and interests of the Company and ensuring the integrity of reporting.

The purpose of this policy is to:

- Facilitate proactive risk management.
- Enhance understanding of all risks faced by Company.
- Facilitate the prioritization of risks.
- Enhance the effectiveness of risk management activities.

This will allow management to make better business decisions through focus on risk & return which in turn will enhance the value for business & preserve its soundness & profitability over time.

Risk Management deals with risks and opportunities affecting value creation or preservation &takes a broad perspective on identifying the risks that could cause an organization to fail to meet its strategies & objectives.

2. Objective

Key objectives of this policy are to:

- Endorse a structured approach to identify current and future potential risks to organization.
- Establish and maintain a system of internal controls to promote effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations.
- Mandate the allocation of each risk to a risk category so that appropriate governance structures and policies & procedures can be developed and implemented.
- Facilitate the making of informed decisions including the prioritization of identified risks consistent with risk tolerance.
- Facilitate the monitoring and reporting on status of all key risks to appropriate management/committees & Board of Directors.
- Provide reasonable assurance with respect to organization’s ability to achieve its strategicand business objectives.

3. Policy Guidelines & Principles

These guidelines recognize that the activities undertaken by organization with respect to the achievement of its strategies and business objectives are ultimately tied to decisions about the nature and level of risk it is prepared to take and the most effective means to manage andmitigate those risks.

The risk management framework which shall govern the related management policies and procedures shall be premised upon common understanding and application of followingprinciples:

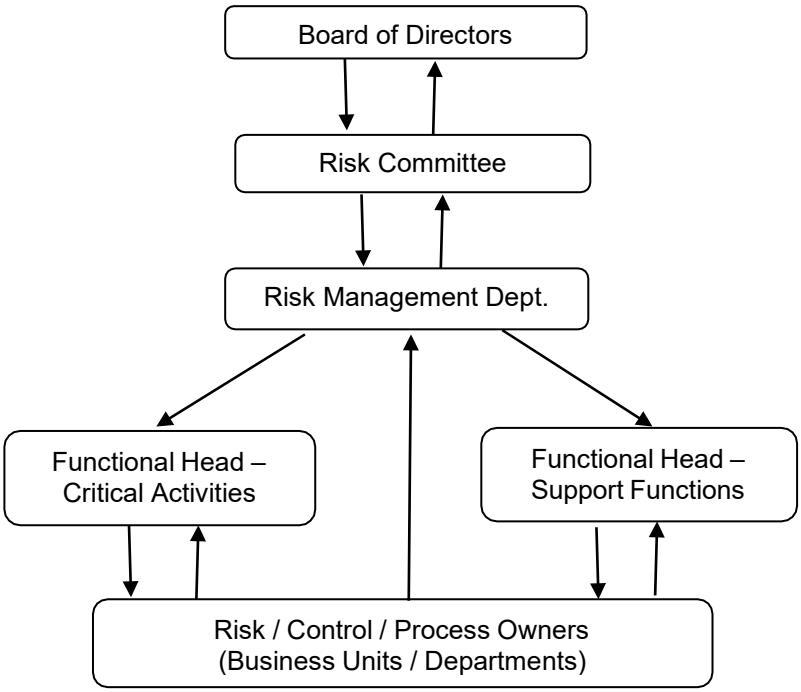
- The informed acceptance of risk is an essential element of good business strategy.
- Risk management is an effective means to enhance and protect the value of businessover time.
- A common definition and understanding of risks is necessary in order to better managethose risks and make more consistent and informed business decisions.
- The management of risk is an anticipatory, proactive process, to be embedded incorporate culture and a key part of strategic planning & operational management.
- All risks are to be identified, assessed, measured, managed, monitored and reported onin accordance with management policies and procedures.
- All business activities are to adhere to risk management practices which reflect effectiveinternal controls that are appropriate for business.

The principles on which this policy document is based and the guidelines set out herein shall be reviewed periodically to ensure that they remain appropriate, in light of changing circumstances and to ensure that such principles and policies are effectively implemented.

4. Risk Organization Structure

A robust organizational structure for managing and reporting on risks is a pre-requisite for an effective risk management process. The risk organization structure for the Company is depicted below:

Risk Management Organization



5. Risk Management Committee

Risk Management Committee is established to assist the Board in its responsibility for ensuring that appropriate risk management and internal control system is in place and for regularly reviewing the effectiveness of same. The Company has framed the risk assessment and minimization procedure which is periodically reviewed by the Audit Committee and the Board. Risk Committee is responsible for monitoring the adherence to the risk policy and guidelines and reviewing the overall risk management system in the light of changes in external and internal environment within which the Company operates.

6. Roles and Responsibilities

i. Role of Board of Directors

The Company's Board of Directors has the responsibility for overseeing all risks associated with the activities of business, establish a strong internal control environment and risk framework that fulfills the expectations of stakeholders of business.

The Board of Directors will review this policy statement on an annual basis, or sooner, depending on the circumstances facing the organization.

ii. Role of Risk Management Committee

The Risk Management Committee provides an overall assessment of risks impacting the activities of the Company and meets on periodic (quarterly) basis or whenever events warrant. The Risk Committee is responsible for the following activities:

- The Risk Management Committee would monitor on overall process of evaluation and assessment, progress of evaluation of control effectiveness, key control deficiencies observedand counter measures to address these. Monitoring would also include significant changes in assessment of key risks or new risks identified, if any.
- Review and approve modifications to existing policies, procedures, and other risk parameters on
  a periodic (at least annual) basis.
- Comprehensive review of this policy document on an annual basis.

iii. Role of Head Risk (CRO)

Head Risk has overall responsibility for the development and implementation of risk control principles,frameworks, limits and processes across all categories of risks faced by organization. A key responsibility of Head Risk includes:

- Providing the overall leadership, vision and direction for risk management.
- Developing risk management policies including the quantification of management's risk appetite.
- Developing risk assessment methodology that is aligned with business objectives at strategic, tactical and operational level.
- Ensuring effective information systems exists to facilitate overall risk management within institution including designing of reporting system.
- Developing the analytical systems and data management capabilities to support risk management.
- To provide periodical updates to Risk Management Committee/Audit Committee/Board on the progress and the implementation of risk management process, key risk identified, and action taken in respect of the same.
- Since the AUM is less than Rs. 5000 crs. the statutory position is left vacant. However, the role of CRO (Chief Risk Officer) is done by Risk manager reporting to CEO (Chief Executive Officer) and Risk management committee.

iv. Role of Functional Heads and Risk and Control Owners

Risk and Control Owners are the personnel who are best placed to influence and manage the risk / control or are best placed to report on the risk/ control. On an ongoing basis, Risk and Control Ownersmonitor their areas for new risks/events or assess changes in risk exposure; as well as carry out periodic assessment of controls in line with the above and report on the same.

Specifically risk and control owners within the business and departments are responsible for:

- Ongoing identification and evaluation of risks within the business and operations;
- Selecting and implementing risk measures on a day to day basis; if any
- Managing certain specified risks under the guidance of the Risk Management Committee;
- Reviewing the effectiveness, efficiency and suitability of the risk management process andaddressing weaknesses;
- Maintaining efficient and cost effective risk handling mechanisms or control framework in line withchanges in the business.

7. Risk Management Process

Risk management process of the Company aims at providing reasonable assurance that the policies and procedures that are in place are adequate considering the scope of business and its activities andare reviewed on an ongoing basis.

Key risk categories for which Company would have policies & procedures in place include:

- Credit Risk including settlement risk
- Market Risk
- Operational Risk
- Fraud Risk
- Legal and Compliance Risk
- Information Security Risk

Extensive and strict norms have been stipulated in identification of the borrower and evaluation of credit proposals. Extensive product programme guidelines have been developed to suit variousproduct requirements. Appropriate delegation and deviation grids have been put in place. Each credit proposal is evaluated on various lending parameters both in qualitative and quantitative terms. Proper security, industry norms and ceilings have been prescribed to ensure well spreading out of risks andto avoid concentration risk. Cross references to credit bureau data are made to assess the credit behaviour of the prospective customers. The credit evaluation process is thus standardized and institutionalized. Market defaulter data are regularly updated through various sources including the Reserve Bank of India (RBI) from time to time and check is done on all applications received. All regulatory requirements are monitored on daily basis and concerned departments are updated for execution.

Risk management process endeavors to identify, assess, monitor and report the risks in terms of above categories with any significant risk being reported to Risk Management Committee. Since the internal and external environment within which the Company operates is exposed to change continuously, the risk management process is kept sufficiently flexible to accommodate new situationsas they arise.

Keeping in view the Directions issued by the Reserve Bank of India (RBI) on Corporate Governance, the Company shall put in place proper risk management mechanism / procedures for complying with the requirements. Necessary reporting and reviewing systems including formation of any Committee shall be established and disclosures made in the Balance Sheet wherever necessary, in line with the requirements of Directions or Rules or Regulations issued or made by any regulatory or statutory authorities, from time to time.

AUTHUM

Fraud Risk Management Policy

Table of contents

1. OBJECTIVE

The Fraud Risk Management Policy has been framed to provide a system for prevention and detection of fraud, reporting of any fraud that is detected or suspected and fair dealing of matters pertaining to fraud.

The policy will ensure and provide for the following:

- To ensure that management is aware of its responsibilities for prevention and detection of fraud and for establishing procedures for preventing fraud and/or detecting fraud when it occurs.
- To provide a clear guidance to employees and others dealing with Company, forbidding them from involvement in any fraudulent activity and the action to be taken by them when they suspect any fraudulent activity.
- To conduct investigations into fraudulent activities.
- To provide assurances that any and all suspected fraudulent activity will be fully investigated & reported.

2. SCOPE OF POLICY

The policy applies to any fraud involving employees of company (all full time, part time or employees appointed on adhoc/temporary/contract basis) and representatives of vendors, suppliers, contractors, consultants, customers, service providers or any outside agencies doing any type of business with the Company.

3. DEFINITION OF FRAUD

"Fraud" is a willful act committed by an individual - by deception, suppression, cheating or any other fraudulent or any other illegal means, thereby, causing wrongful gains to self or any other individual and wrongful loss to others. Many a times such acts are undertaken with a view to deceive/mislead others, leading them to do or prohibiting them from doing a bonafide act or take bonafide decision which is not based on material facts. Frauds have been classified as under based mainly on the provisions of theIndian Penal Code as specified by Reserve Bank of India vide its circular DNBS.PD.CC. No. 256
/03.10.042 / 2011-12 dated March 02, 2012.

- Misappropriation and criminal breach of trust.
- Fraudulent encashment through forged instruments, manipulation of books of account or throughfictitious accounts and conversion of property.
- Unauthorised credit facilities extended for reward or for illegal gratification.
- Negligence and cash shortages.
- Cheating and forgery.
- Irregularities in foreign exchange transactions.
- Any other type of fraud not coming under the specific heads as above.

An effective, business-driven fraud risk management approach is one that isfocused on three objectives:

- **Prevention** controls designed to reduce the risk of fraud from occurringin the first place.
- **Detection** controls designed to discover fraud when it occurs.
- **Response** controls designed to take corrective action and remedy the harm caused by fraud .

4. FRAUD PREVENTION

Preventive controls are designed to help to reduce the risk of fraud and misconduct from occurring in thefirst place. These controls are categorized based on:

- Governance
- Roles and Responsibilities
- Internal Audit Function
- Fraud risk assessment

i. Governance based Fraud Prevention

ControlsCode of Conduct

Company's code of conduct is one of the most important communications vehicles that management usesto communicate to employees on key standards that define acceptable business conduct. Code of conduct in place is based on below key attributes:

- High-level endorsement from the organization's leadership, underscoring a commitment to integrity
- Simple, concise, and positive language that can be readily understood by all employees
- Ethical decision-making tools to assist employees in making the right choices
- A designation of reporting channels and viable mechanisms that employee can use to report concernsor seek advice without fear of retaliation.

Employee & Third Party Due Diligence

- An important part of an effective fraud prevention strategy is the use of due diligence in the hiring, retention, and promotion of employees, agents, vendors, and other third parties.
- Due diligence begins at the start of an employment or business relationship and continues through out. For instance, taking into account behavioral considerations such as adherence to

the organization's core values in performance evaluations provides a powerful signal that management cares about not only what employees achieve but also that those achievements were made in amanner consistent with the company's values and standards.

Communication and Training

Making employees aware of their obligations concerning fraud prevention control begins with practical communication and training. In formulating a training and communications plan, the Company will consider developing fraud awareness initiatives that are:

- Comprehensive and based upon job functions and risk areas.
- Integrated with other training efforts, whenever possible.
- Regular and frequent, covering the relevant employee population.

Training can help to raise staff awareness of the risks of fraud and the importance of compliance with internal control procedures and security checks to prevent such frauds. And close monitoring of staff compliance with these controls helps ensure their consistent application.

Whistle Blower Policy & Mechanism

The Company has formulated a Whistle Blower policy & put in place Ombudsperson mechanism for administration of the process. The Company encourages the "Speak-Up" culture for disclosing in goodfaith any wrongful conduct on matters of public concern involving violation of any law, mismanagement, fraudulent practices, gross waste or misappropriation of funds. The Company maintains the confidentiality of the whistle blower and ensures no retaliation or adverse action initiated against them who disclose the details in good faith.

ii. Roles & Responsibilities Board Oversight

Board of Directors of the Company plays an important role in the oversight and implementation of controls to mitigate the risk of fraud. The Board, together with senior management, is responsible for ensuring that appropriate internal controls and risk management system is in place & to regularly review the effectiveness of same.

The board has delegated principal oversight for fraud risk management to Risk Management Committee(RMC), which is tasked with, among other things:

- Reviewing and discussing the internal and external auditor's findings on the quality of theorganization's antifraud controls and checks.
- Periodically reporting to Board on occurrence of fraud incident and required action taken.

Board is responsible for administration, interpretation, application and revision of this policy. The policywould be reviewed and revised annually or in exceptional circumstances as and when needed.

Risk Management Committee

The Risk Management Committee (RMC) is responsible for this policy and will maintain, interpret andcommunicate the policy in Company. The Committee is responsible for the following activities:

- To initiate and oversee a prompt investigation of any suspected fraudulent act or omission or non-compliance with the policy's requirement.
- Review the issues identified during entity's fraud risk assessment as well as during internal andexternal audit.
- To ensure that this policy and related guidelines are communicated, updated and made available to allemployees and representatives within Company.
- To ensure that Board of Directors are informed on occurrence of any fraud incident through periodicalreporting process.

To review the fraud incidents at the Company and to ensure the compliance of this policy, any fraud incident at the Company will be reviewed in Operational Risk Management Committee (ORMC). The minutes of the ORMC meeting will be placed to RMC meeting.

Risk Containment Unit (RCU)

To help & ensure that fraud prevention controls remain effective and in line with standards, Risk Containment Unit (RCU) will be responsible for the Company's fraud risk management. Direct responsibility for antifraud efforts would reside with a RCU - Head, who will work in co-ordination withother operational & support functions as may be required. While discharging its function, RCU inter-alia adopts the following proactive fraud risk management strategy:

a) **Understanding and Profiling** – **K**nowing **Y**our **C**ustomers and **V**endors by means of evaluation, verification, detailed checks of their financial and business conditions before getting into a relationship with them.

b) **Deterring Fraud** - Conduct fraud awareness trainings across organisation so as to create a general awareness amongst all groups/vendors, informing them about the general frauds prevailing in the market and the consequences of getting involved in a fraud.

c) **Preventing Fraud** -
   - Use various techniques like Intelligent Seeding/Mystery Shopping;
   - Cross verification of reports (Field Investigation / Document Verification / Technical

Reports / Legal Reports / Valuation Reports) to proactively prevent frauds.

- Networking with Financial Institutions/Law enforcement agencies/Insurance companies/Telecom companies etc., so as to proactively gather information about latest market happenings which would subsequently help in preventing frauds.

d) **Detecting fraud** –
   - Applicant fraud is detected by a process called Application Sampling – Physical and Transaction exception monitoring through a Fraud rule engine. Sampled applications are further used to detecta false positive or a confirmed fraud.
   - Additionally, as a support to detect fraud there is a Strong and Dynamic In-house Negative Database with a dedupe engine.
   - Usage of CIBIL (Credit Information Bureau of India Ltd.) for Velocity Monitoring.
   - Post Disbursal Asset Verification is being conducted on a sample basis to detect whether any asset fraud has happened.

e) **Investigating Fraud** – Conduct investigations on confirmed frauds to identify loopholes in process, systems and people compromise so as to plug these loopholes.

f) **Sanctions** – Post investigations of fraud, identify erring parties who have perpetrated the frauds and initiate measures for levying necessary penalties or blacklist them and for other actions including disciplinary actions and reporting & resorting to law enforcing agencies.

g) **Redress** – Findings from Fraud Investigations are quickly downloaded to the Policy, Underwritingand other relevant teams so as to avoid the same kind of frauds hitting the system.

In terms of Process, this is achieved by doing:

- Vendor evaluation
- Two tier Trigger Based application sampling – Physical and Transaction exception monitoring througha Fraud rule engine.
- Validation services – Profile and Documents
- Strong and dynamic Negative Database
- CIBIL – Velocity monitoring
- Market information
- Post Disbursal Asset Verification
- Intelligent Seeding
- Mystery Shopping
- Cross verification of reports (FI/Document verification/Technical/Legal/Valuation/Site visits)
- Networking with Financial Institutions/Law enforcement agencies/Insurance companies/Telecomcompanies etc.
- Fraud Investigation
- Fraud awareness trainings

- Setting deterrents

Functional Heads, Employees and Representatives

- All functional heads shall share the responsibility of prevention and detection of fraud. It will beensured that there are mechanisms in place within their area of control to:
  a. Familiarize each employee with the types of improprieties that might occur in their area.
  b. Educate employees about fraud prevention and detection.
  c. Create a culture whereby employees are encouraged to report any fraud or suspected fraud whichcomes to their knowledge, without any fear of victimization.
  d. Help in minimizing the impact of fraud and mitigating the loss arising out of it.

- Every employee (full time, part time, adhoc, temporary, contract), representative of vendors, suppliers, contractors, consultants, service providers or any other agencies doing any type of business with the company is expected and shall be responsible to ensure that there is no fraudulent act being committed in their areas of responsibility/control. As soon as it is learnt that a fraud or suspected fraud has taken or is likely to take place they should immediately apprise the same to the concerned as per the procedure.

iii. Internal Audit Function

Internal audit would be responsible for:

- Planning and conducting the evaluation of design and operating effectiveness of anti-fraud controls.
- Assisting in the organization's fraud risk assessment and helping draw conclusions as to appropriatemitigation strategies.
- Reporting to the Risk Committee on internal control assessments and related activities.

iv. Fraud Risk Assessment

Fraud risk assessment helps to understand the risks that are unique to the business, identify gaps or weaknesses in control to mitigate those risks, and develop a practical plan for targeting the right resourcesand controls to reduce risk.

It would be ensured that such an assessment is conducted across the entire organization as a part of overall enterprise wide risk review plan, taking into consideration the entity's significant business units, processes, and functions.

With input from process owners as to the relevant risks to achieving organizational objectives, a fraud risk assessment includes the steps listed in below diagram:

5. FRAUD DETECTION

Detective controls are designed to uncover fraud when it occurs. Frauds are detected by various belowmethods among others:

- Whistle blower Policy
- Internal or external tip-off
- Hindsight and risk reviews
- Audit: Internal / External
- Customer Complaints
- Negative customer data
- Investigation based on regulatory requirements
- Periodical evaluation of external vendor both pre and post empanelment
- Document/Asset Verification

i. Internal Control and Continuous Monitoring

Internal control measures and monitoring systems that are reasonably designed to detect fraud are important tools that management uses to determine whether organization's controls are working as intended. Management develops a comprehensive internal control and monitoring plan that is based on risks identified through the organization's fraud risk assessment process.

An internal control and monitoring plan would thus encompass activities that are tailored in depth to the nature and degree of the risk involved, with higher-risk issues receiving priority treatment. Internal control review activities (an evaluation of past events) and monitoring activities would be performed in, but are notlimited to, areas where:

- There are specific concerns about a key process or function
- The company has a history of occurring fraud in respective area
- There is high employee turnover or organizational change

- Laws and regulations have changed significantly

The effectiveness of the internal control systems & monitoring mechanisms are subjected to independent evaluation by the internal audit.

ii. Proactive Data Analysis

Many of the indicators of fraud, both actual and potential, reside within an organization's financial, operational, and transactional data, and are identified using data analysis tools and techniques. Such proactive data analysis is based on analytical tests, computer-based cross matching, and non-obvious relationship identification to highlight the potential fraud. Techniques such as data matching, generating alerts etc., used for analyzing the data. Benefits of such an analysis includes, among others:

- Identification of hidden relationships between people, organizations, and events
- A means to analyze suspicious transactions
- An ability to assess the effectiveness of internal controls intended to prevent or detect fraudulentactivities
- The potential to continually monitor fraud threats and vulnerabilities

iii. Reporting of Suspected Fraud

- With the oversight and guidance of senior management, Company should provide employees withmultiple channels for reporting concerns about fraud.
- When an employee or representative suspects that a fraudulent act has occurred, he or she should report this immediately to his/her immediate supervisor. If the employee or representative does not feel comfortable reporting to his/her superior, he/she should directly report to the **Risk Office (Head – Risk Containment Unit or Chief Risk Officer)**. He or She can also report to Ombudsperson as per Whistle Blower Policy.
- The Risk Officer may communicate such incident to relevant functionaries depending upon the exigencies, at his/her discretion. The reporting person's identity in any follow up discussion or enquiries should be kept in confidence to the extent appropriate and permitted by law.
- Officer receiving input about any suspected fraud should ensure that all relevant records, documents and other evidence is being immediately taken into custody and being protected from being tampered, destroyed or removed by suspected perpetrators of fraud.
- A mischievous or malicious allegation of fraud or suspected fraud will constitute a breach of the code of conduct. Any reprisal, retaliation or disciplinary action against employee or representatives for reporting suspected fraud in good faith should be prohibited.

6. FRAUD RESPONSE

Response controls are designed to investigate and take corrective action to remedy the harm, caused byfraud.

i. Investigation

When information relating to actual or potential fraud is uncovered, management conduct a comprehensive investigation with the objective to:

- Assess and document the facts of case, prevent the fraud from continuing and to protect the innocent.
- Provide basics for appropriate consequences, upto and including the termination of employment orcontract and taking legal action where appropriate.
- Taking legal actions against the culprits if necessary.
- Recovery of loss if any suffered for fraudulent act.
- Improve the controls to prevent the future fraudulent acts.

Investigation is highly sensitive, and it is therefore critical that it is conducted in a prescribed manner involving only those people who require the information to conduct a proper investigation. Further, it is conducted in accordance with applicable laws and the rights as well as privacy of all parties involved should be respected to the extent required.

Below is brief about investigation process:

- Head - RCU before initiating any investigative action should consult CEO for determining the courseof action. Other departments to be consulted on need to know basis only.
- Wherever need be a team of officials can also be formed for conducting such investigations.
- The means to carry out the investigation should be within the bounds established by law.
- The investigation should be conducted diligently with high professional standards without any bias.
- All investigation should be carried out in an independent manner with due regard for the individual's rights but without regard to length of service, position held or relationship with the company.
- All investigation must be kept confidential. Information related to the suspected fraud may not be revealed other than to the functional heads of the finance team, human resources team, and legal team, senior management and or others on a need to know basis.
- Care must be taken in an investigation of suspected fraud to avoid mistaken accusations or alerting suspected individuals that an investigation is underway.
- The result of investigations should be disclosed by the investigating officers to only those individuals who require the information to perform their roles.
- Investigation should be completed within the reasonable time frame.

- Investigating officer / team to submit comprehensive report including the modus operandi, people behind the perpetration of fraud, traces of frauds, gaps in the systems & processes, gaps in adherence & compliance, primary & contributing factors leading to such frauds, suggestions forstrengthening the systems & plugging the gaps.
- Submission of interim or flash reports apprising the status may also be considered as & when felt necessary.
- The report should be, wherever necessary, supported & substantiated by evidences, disclosures, confession statements, statement by witnesses. All the material & documents collected prior & during the investigation should be kept confidential & under proper custody of Head – Risk Containment Unit or nominated persons.
- The findings of the investigation need to be discussed out with all concerned for ensuring cross sectional views and for addressing the other requirements.
- Incidents of fraudulent acts or omissions should be reported to appropriate regulatory and/or law enforcement agencies if same is the requirement.
- History of all the investigations needs to be maintained & tracked.

ii. Corrective Action

A consistent and credible disciplinary system is a key control for deterring fraud. Well-designed disciplinary process is communicated to all employees and external parties to ensure that all concerned are aware about consequences in terms of verbal warning, written warning, suspension, pay reduction, location transfer, demotion, termination, taking legal action or imposing financial penalty.

Once fraud has occurred, management considers taking action to remedy the harm caused. The Company considers fraudulent activity to be a very serious offence. Actions up to and including termination of employment or contract for just cause should be pursued when warranted. In addition, the Company:

- May take action to recover losses incurred as a result of fraudulent acts or omissions; and
- May refer the matter to law enforcement, regulatory agencies or external organizations for thepurpose of further investigation or prosecution.

In no circumstance will any decision be taken to discipline, suspend or terminate an individual's employment or contract without notification to, and approval of head of human resources function. Furthermore, matter will be referred to law enforcement, regulatory agency or external organization for thepurpose of further investigation or prosecution with the approval of Chief Executive Officer, Risk Management Committee Head and Compliance Officer. In case of exigencies action can be taken with the approval of any of the above.

7. REPORTING

Fraud incident reporting requirements are based on circular issued by Reserve Bank Of India (RBI) on September 23, 2003 vide reference no. RBI (ND)/RCF/(P&D)/2391/2003 or as may be issued from time- to-time. Accordingly, reporting is to be done as below:

Reporting to RBI DNBS.PD.CC. No. 256/03.10.042 / 2011-12 dated March 02, 2012.

i. Report on occurrence of fraud incident

- Company should report fraudulent transactions as and when detected to RBI immediately and in any case not later than three weeks from the date of detection as per the format prescribed by RBI in Annexure 1 of above mentioned circular.
- The reporting contains brief particulars of the fraud such as:
  - ✓ Branch in which the fraud occurred
  - ✓ Name and address of party in whose account the fraud occurred
  - ✓ Date of occurrence and date of detection
  - ✓ Estimated loss
  - ✓ Nature of fraud
  - ✓ Modus Operandi in brief
  - ✓ Serious irregularities observed
  - ✓ Steps taken / proposed to be taken to avoid such incidents

ii. Report on Follow Up

Company is also required to send detailed information to RBI regarding the action taken by on the fraudulent cases within six months from the date on which the fraud was detected as per the format prescribed in Annexure 2 of above mentioned circular.

A. Reporting to Board

- Company will report to Board on all fraud incidents promptly on their detection.
- Company will conduct an annual review of the frauds and place a note before the Board of Directors. Review will be done for upto period ended December in respective financial year and will be put up to Board before the end of March of following year. Key aspects that will be covered as a part of review will include:
  - ✓ Whether the systems in place are adequate to detect frauds, once they have taken place, within the shortest possible time.
  - ✓ Whether frauds are examined from staff angle.
  - ✓ Whether deterrent punishment is meted out, wherever warranted, to the persons found responsible.

- ✓ Whether frauds have taken place because of laxity in following the systems & procedures and if so, whether effective action has been taken to ensure that the systems & procedures are scrupulously followed by the staff concerned.
- ✓ Whether frauds are reported to local Police, as the case may be, for investigation.

B. Reporting to Police

- In the following scenario, cases will be referred to Local Police depending upon the severity and natureof fraud. Such referrals to local police will be at the joint discretion of the Risk Head, Human Resources (HR) Head & CEO.

  - ✓ Cases of fraud committed by employees, when it involves funds exceeding Rs.10,000/-.

8. ANNEXURE

Below annexures are attached to this Fraud Risk Management Policy:

- **Annexure - I** : Annexure 1 (Reporting to RBI - Details of Fraudulent Cases Detected)
- **Annexure - II** : Annexure 2 (Reporting to RBI - Details of Fraudulent Cases - Follow Up)

Annexure - I

Annexure 1: Details of Fraudulent Cases

DetectedName of the NBFC:

Certificate of Registration (Number):

1.	Name of the Branch in which the fraud occurred	
2.	Name & Address of the party in whose account the fraud occurred	
3.	If a builder loan, details of the proprietors/partners/directors	
4.	Name & Address of associate concerns	
5.	Nature of account	
6.	Date of sanction	
7.	Date of occurrence of fraud	
8.	Date of detection	
9.	Estimated loss to the HFC	
10.	Nature of fraud (in detail indicating specific instances of fraudperpetrated by the concerned party) (modus operandi, serious irregularities, etc.)	
10 (i)	Modus Operandi	
10 (ii)	Serious irregularities observed	
10 (iii)	Causative factors	
10 (iv)	How fraud was detected?	
11.	Steps taken/proposed to be taken to avoid such incidents	

CEO / CFO

Date:

Annexure - II

Annexure 2: Details of Fraudulent Cases - Follow Up

(Quarterly Report for the quarter ended_____)

Name of the NBFC:

1.	Date of first reporting and amount involved.	
2.	Branch in which fraud occurred.	
3.	Name & Address of the party in whose account the fraud occurred.	
4.	Date of Reporting to the Board of Directors of the company.	
5.	i. Whether criminal complaint filed with CBI/Police. If so, give name of branch/office of CBI/Police, date of reference and present position of the case. If not, reasons therefore. ii. Date of filing of civil suit against the concerned borrower and further developments in the matter. If not, reasons therefore. iii. Whether the HFC has conducted departmental enquiryin the matter and examined the staff side of the case. Ifnot, state reasons. iv. Progress/Position of Departmental Enquiry against each member of staff involved. v. Punishment awarded (with names, designation and nature of punishment) vi. Prosecution/conviction/acquittal etc. in respect of officials involved with details.	
6.	Action taken/proposed to be taken by the NBFC against the staff responsible for the lapses.	
7.	The date on which last internal inspection/audit was conductedat the branch during the period between the date of first occurrences of the fraud and its detection.	
8.	Any other Developments.	

Note: Information to be furnished within six months from the date on which the fraud was detected inrespect of each fraud.

****