# “Preventive Vigilance Framework with Special Emphasis on Activation & Promotion of Whistle Blower Policy”

## 1. Background of the Proposed Framework.

1.1. Main Highlights of Fraud Surveys. Different surveys conducted to estimate the extent and impact of various fraud incidents on business organizations and the society, have revealed that fraud incidents, a hard reality, are faced by most of the organization across the globe and it continues to remain a serious and costly threat to their smooth working. According to Earnest & Young[1] ―the current economic pressures have increased incentives to act unethically. There remains a real need for companies and those charged with their governance and oversight to revisit their focus on the risks of fraud‖. The risks of

fraud are likely to increase with growing globalization, more competitive markets, rapid developments in technology and periods of economic difficulty. Various surveys conducted globally have **highlighted**:

a) that organizations may be losing as much as 7% of their annual revenue/ turnover in fraud incidents;
b) that corruption is estimated to cost the global economy about $1.5 trillion each year;
c) that only a small percentage of losses from fraud are recovered by organizations;
d) that a large number of frauds are committed by insiders;
e) that greed is one of the motivators for committing fraud;
f) that fraud losses are not restricted to a particular sector or country; and
g) that the prevalence of fraud is now increasing in emerging markets of world economy.

1.2. **Purpose**. ―Preventive Vigilance Framework with Special Emphasis on Activation & Promotion of Whistle Blower Policy[2]‖ defines the governance, roles & responsibilities of various officials/ officers from a business unit to the Board level together with putting in place various controls for preventing fraud incidents and detecting frauds in an effective way. It also aims at setting various controls for fraud risk management at different levels in the organization.

1.3. **Objectives**. The objectives of the framework are :

a) to ensure that the policies and procedures are consistently and effectively applied/ followed in the bank and supervised/ monitored effectively ;
b) to define and demarcate the responsibilities of the staff who are one of the major stakeholders in fraud prevention at various levels of hierarchy;
c) to set out the requirements for the need to implement and monitor a proactive framework on prevention of fraud incidents in sync with the regulatory compliance so that the business goals and compliance issues move in close coordination; and
d) to implement a fraud risk management framework focusing on areas that entail higher risk.

1.4. **Commitment of the Bank to a Fraud-free Organizational Set-up.**

1.4.1.The bank has a commitment to strive for a fraud-free organizational set-up with best possible systems and procedures and fraud mitigation measures with high legal, ethical and moral standards. All stakeholder in general and employees of the bank , in particular are expected to demonstrate this commitment. Existing procedures for achievement of this objective include documented processes and systems of internal control, risk assessments at different levels and inculcation of fraud awareness culture by clear communications/ awareness from time to time including sharing of modus-operandi of various fraud incidents.

1.4.2. This document is intended to provide direction to the staff to deal with suspected cases of theft, fraud and corruption for moving towards a fraud-free environment. The document gives a *broad framework* on various aspects on both suspected/ actual fraud-prone areas and steps to detect fraud incidents effectively and proactively rather than responding in a reactive (passive) way.

[1] 15th Global Fraud Survey 2018 : Integrity in the spotlight The future of compliance [2] For brevity referred to as ―Framework‖ henceforth.

1.5. **Comprehensive Coverage of the Preventive Vigilance Framework**.

This policy framework applies to any irregularity, or suspected irregularity, involving employees as well as consultants, suppliers, contractors, and/or any other parties having a business (transaction-based as well as on-going) relationship with the bank. Any investigation required will be conducted without regard to any person‘s relationship to the organization, position or length of service.

1.6. **Actions Constituting Suspected Fraud & Role of Bank‟s Staff.**

For the purpose of determining a fraud event, besides regulatory/ legal and other extant guidelines, the use of deception to obtain an unjust or illegal financial advantage and intentional misrepresentations, by one or more individuals among employees or third parties, affecting the relationship of the bank with any of its constituents/ stakeholders. All staff, irrespective of their positions, have a duty to familiarize themselves with the types of improprieties that might be expected to occur within their areas of functioning and to be alert for any fraud-incident indications/ irregularity. Should they at any point of time reasonably suspect that a fraud event is in the offing or likely to occur, they must report it to the

next/ top levels of management of the bank as responsible employees either directly or by using whistle-blower mechanism.

1.7. **Strategy of Preventive Vigilance Framework: Broad Aspects.**

The strategy under the ―Framework‖ would broadly be based on following aspects:

a)To consider fraud risk as an integral part of overall corporate risk management strategy.

b) To develop an integrated strategy for prevention and control of frauds.

c) To develop an ownership structure from the top to the bottom of the organization.

d) To introduce a fraud policy statement.

e) To introduce an ethics policy statement.

f) To promote these policies throughout the organization.

g) To establish a fraud control environment throughout the entire organization.

h) To establish sound operational control procedures.

i) To introduce fraud education, training and awareness programs.

j) To introduce a fraud response plan as an integral part of the organization's contingency plans.

k) To frame & operationalize a whistle-blowing mechanism as a part of overall _Fraud Risk Management Strategy.'

k)To put in place a *Reporting Hotline for Escalating Suspected/ Real Fraud Incidents* and Other similar Misdemeanors. This job will be either outsourced or assigned to the In-charge Vigilance Department (a Scale 3 or Scale 4 officer).

l) To periodically review all anti-fraud policies and procedures.

m) To establish a ―Learn from Experience Data Base for not repeating the Similar-Reported Fraud Events‖ (this is done by **putting a compendium of fraud-incident circulars** on the intra-net of the bank).

n)To develop an effective & appropriate communication system for prevention, detection, reporting, investigation and assessment of fraud incidents.

## 2. Risk Appetite of the J&K Bank for Fraud Incidents & Functional Role of 3 Defence Lines.

2.1. Generally, the main mantra for any organization's ―fraud risk appetite‖ is based on **two principles** i.e. (i) some tolerance for external fraud owing to business dynamics and (ii) no/ zero tolerance for internal frauds. However, there is some gap between these stated tolerance levels and the actual fraud incidents in view of dynamics of the business reality and the efficacy of execution of fraud-riskframework with the use of best available high-tech solution for managing ―Fraud Risk Framework‖ which is in the offing and would take a few months to operationalize. Although efforts to plug the loopholes in the existing systems are a continuous process, yet strict enforcement of existing controls/ systems and compliance to the extant guidelines needs conscious improvement for moving towards the goal of a *near* fraud-freed banking business environment. To adequately manage internal frauds, close alignment is also required between prevention, detection and mitigation processes within the overall risk appetite of the bank. Despite clear resolve that the bank & its staff would strive for a fraud-free internal environment, it is, at times, observed with dismay that involvement of a small fraction of staff in perpetration of internal-fraud continues. This is obviously a serious concern. *Hence, with the resolve of the top management & the entire staff at operational levels there would be zero / no tolerance for internal frauds and the bank is committed to root out all such tendencies that show any inclination for perpetration of a fraud incident. These tendencies of any miscreant will be dealt with an iron hand without any sympathy/ clemency*. **We may, for quantifying the riks-appetite take the average amount of last three years fraud incidents as the overall risk appetite of the bank.**

2.2. Secondly, with stronger regulatory supervision , the banking system in India is continuously evolving to a ―mature fraud risk operating model‖ and our bank is on the fore-front in implementing all possible sound policies and fool-proof systems to reduce the impact of external frauds. As the **implementation of "Enterprise-wide Fraud Risk Solution (EFRS)" for Vigilance functions in near future by Strategy & IT Department, is likely to include all critical areas including the entire credit portfolio for monitoring of early fraud-alerts** . Till such time the EFRS is made operational, the bank would strive to manage the best possible balancing-blend between the customerservice-satisfaction and business growth with focus on reducing of fraud-risks. Our customers in general and high-end customers, in particular, would be facilitated by best customer services/ experience with high degree of convenience in a fraud-free environment.

2.3. Three Lines of Defence for Managing Fraud Risks. Generally, management of fraud risk has to be well-defined/ well-documented at various levels of the hierarchy and locations within the organization and allocated to different individuals or departments as per their respective job roles. Hence, for effective

management of fraud risk framework (prevention, detection, response and remedial measures) the ***three lines of defence*** within the bank with their respective role is given under:

2.4. First Line of Defence. The first line of defence at the operational level, branch and concerned support/ back offices (including RCC's) would constitute all staff members who have different job roles for various banking operations on day-to-day basis. They will be solely responsible for ownership, responsibility and accountability for mitigating the occurrence of fraud incidents within their designated job-roles by complying with the extant systems & procedures. An illustrative (but not exhaustive) check-list of different vulnerable areas is given in table at Para 6 of this framework. It is obvious that the first responsibility to manage fraud risk lies with the **operational verticals** as they are directly associated with the banking processes and their vulnerabilities , the products and their risk-factors and customers and their banking habits. They are/ will be the first to react/ respond. **To enable them to perform this role it is necessary** :

- That the staff at operational level receive proper training to recognize a fraud incident and respond to it properly/ professionally *.( It will be joint responsibility of both Vigilance Department and HRD, Corporate Headquarters to impart requisite training & awareness for improving the skill-sets of the staff at operational levels*);
- That adequate preventive and detective control measures are in place and functional. *(This will be sole responsibility of the Vigilance Department to arrange to put in place proper preventive and fraud detection measures from time to time so that the staff at operational level is well informed about these measures);*
- That fraud incidents are identified and investigated. *(The investigation of fraud incidents will be got conducted by the Vigilance Department, Corporate Headquarters either through Divisional S&C's or with its own staff or some outside agencies after proper internal approval depending on the seriousness and sensitivity of a fraud incident to be investigated);*
- That loopholes/ learning points from a fraud incident are documented and shared with the operational levels for raising the awareness level of the staff and for preventing recurrence of similar incidents . *(The Vigilance Department would continue to share through internal circulars/ communications the modus-operandi of various fraud incident and suggest measures for plugging the loopholes/ lacunae in the system & procedures)* ; and
- That staff side action and/ or legal action is taken expeditiously within the regulatory time-line *(S&C, and Vigilance Departments , Corporate Headquarters would examine each case for staff-side action besides pursuing the fraud incidents for filing of FIR with police/ in court till final closure of police case or awarding of court verdict as per the RBI directions).*

It is clear that that the staff on the first line of defence must take up their role / responsibility and show concern to mitigate the fraud risks.

2.5. Second Line of Defence. The second line of defence would constitute the Cluster/ Zonal and S&C Divisions whose role is to offer supportive services to the staff posted at First Line and they would be driven by the goal of business growth with efficacy of systems at operational level. They would be overseeing, facilitating and monitoring the implementation of effective risk management practices besides assisting the fraud-risk owners (Corporate Headquarters and other level in the organization) in reporting risk-related events/ incidents/ information in both up-and-down directions in the organization. It will be responsibility of the second line to ensure that an adequate and consistent approach is pursued to de-risk the impact of fraud incidents and maintain oversight on operational aspects to report possible risks from time to time and suggest measures for improving the efficacy of the bank's fraud defence systems within their respective areas. . **To enable them to perform this role it is necessary:**

- That proper fraud prevention framework is made operational by the Vigilance Department and the same is communicated to the operational/ other levels;
- That they would maintain proper contact/ communication with the top management and assist them in operationalization of this framework; and
- That fraud detection measures/ controls whether manually or through technological-intervention are developed/ communicated and implemented.

2.6. Third Line of Defence. The third line of defence in the bank, constituting inspectors and auditors working under the direct control of S&C Divisions/ Compliance Departments / Zonal Offices, would through a risk based approach / reporting system provide timely feed-back/ inputs and assurances to the top management of the bank including the ACB/ Board on efficacy and effectiveness of fraudrisk measures from time-to-time for arresting occurrence of fraud incidents and mitigation of fraudrisks on

both liabilities and assets side of the balance sheet of the business unit/ bank. They would also provide information about the working of the first and second lines of defence. To ensure proper management of fraud risk and to maintain coherence with other risk management processes, alignment of different components of fraud risk would be monitored at by the S&C Corporate Headquarters and Vigilance Departments as per their respective functional roles. The role of the internal audit/ inspection system in mitigation of fraud risk would be limited to providing assurances that the first and second lines of defence are functioning properly and that specific fraud vulnerability areas have been adequately addressed. However, internal audit/ inspection system would avoid starting any inquiry on its own.

**3. Anti- Fraud Measures: Bank Presently in Progressive / Evolutionary Mode.**

To take forward the present fraud deterrence measures, the bank would progressively move towards a comprehensive/ mature system of anti-fraud controls for reducing fraud risks and fraud losses, curtailing the time-lag in detection of fraud incidents. The various *anti-fraud controls & their present status of operational use* are tabulated below:

| S. No. | Fraud Control Measures | Status of their Operationalization |
|---|---|---|
| 1. | Formal Anti-fraud policy | Already in use & circulated vide ―Policy Framework on Fraud Risk Management & Vigilance (2017-18 Version)‖ in March, 2018. |
| 2. | Dedicated fraud detection, investigation, reporting Department | Vigilance Department assigned this job |
| 3. | Formal Fraud Risk Assessment of Business units/ Operational Office and at Enterprise-wide level | Fraud Prevention/ Score Card/s introduced. However, use of Artificial Intelligence and Technology-based Fraud Risk Solution in prevention, detection, analysis and reporting of frauds is under process through the T&IS Department, Corporate Headquarters. |
| 4. | Hotline/ Whistle Blower Mechanism for escalating Fraud Incidents. | Hotline proposed as at Para 1.7 (k). However the whistle blower mechanism is already in existence. |
| 5. | Management Review of Fraud Incidents | Done by the ACB/ Special Committee of Board for Fraud Review/ Board. |
| 6. | Training/ Awareness Programs on Prevention of Frauds | Staff is presently updated about various fraud incidents in the banking industry through different circulars and by sharing of modus-operandi of fraud incidents on an on-going basis. Their training requirements will be looked into separately by the Vigilance/ Human Resources Departments Corporate Headquarters. |
| 7. | Pro-active Data Monitoring / Analysis | Will be taken over once the measures given at para 3 (use of Artificial Intelligence and Fraud Risk Solution ) are in place. |
| 8. | Formal Code of Conduct | Already circulated vide ―Policy Framework on Fraud Risk Management & Vigilance (2017-18 Version)‖ in March, 2018. |
| 9. | Surprise/ Forensic Audits | Presently Risk Based Internal Audit (RBIA) is done through the S&C, Corporate Headquarters. Besides other regulatory audits like Concurrent Audit and classification of accounts as ―Red Flag Accounts‖ for fraud signals is done through the A&AP Department. Special/ Forensic Audits are got conducted on case-to-case basis as per the recommendations of Credit Monitoring Committee, CHQ. |
| 10. | Job Rotation / Mandatory Leave of staff in Key Functional Areas | Instructions already issued by the HRDD, Corporate Headquarters on it. |
| 11. | Rewards for Genuine Whistleblowers | We may incorporate it in the Whistleblower Policy which is under review with this ―framework‖ |
| 12. | Zero-tolerance for Fraud Incidents | To be embedded in the business operations gradually as presently fraud management processes are manual and not system driven. |

<table>
<tr><td>13.</td><td>Effective Monitoring Mechanism for on-line/ other frauds through:<br>i) Fraud Review Council;<br>ii) Fraud Risk Management Group<br><br>for overall responsibility for ―Fraud Response‖ for the bank.</td><td>Both the forums for monitoring of frauds i.e. Fraud Review Council (FRC) and Fraud Risk Management Group (FRMG) are already in place but their efficacy/ effectiveness needs further improvement so that they are fully equipped and made responsible for framing/ implementing desired ―Fraud Response‖ plan as & when the need arises.</td></tr>
<tr><td>14.</td><td>Functional Specific Approach to prevention and detection of frauds</td><td>Proposed to be introduced vide this framework.</td></tr>
<tr><td>15.</td><td>Risk focused Approach to Fraud Management</td><td>To introduce ownership of fraud-risk by risk category , it is proposed to associate a cross-section of departmental heads in this role as per their respective functional areas detailed below:
<table>
<tr><th>Fraud Risk Category</th><th>Ownership with Departmental Heads</th></tr>
<tr><td>Fraud risk from Compliance Issues</td><td>Chief Compliance Officer (CCO) of the bank</td></tr>
<tr><td>Isolating staff with Corrupt tendencies and/ or having record of corrupt-practices from sensitive positions/ posts and maintenance of their proper record.</td><td>Executive President (HRDD) or any other top executive heading the HRDD.</td></tr>
<tr><td>Loss to Physical Assets and Security</td><td>President (S&IT)/Security Officer</td></tr>
<tr><td>Capturing fraud disclosure data and level of provisions in Financial Reporting</td><td>Chief Financial Officer (CFO) of the bank</td></tr>
<tr><td>Vigilance Issues/ Aspects</td><td>CVO</td></tr>
<tr><td>Anti-trust/Legal Issues</td><td>President/ Vice President , Law Department, CHQ</td></tr>
<tr><td>Periodic Assessment of ―life style‖ of staff and maintenance of records thereof.</td><td>Zonal Heads within their respective areas and Vice President (HRD, CHQ) for staff posted in Zonal Office/ Corporate Headquarters.</td></tr>
</table></td></tr>
</table>

## 4. Fraud Risk: An Integral Part of Overall Corporate Risk Management Strategy.

### 4.1. What is a Fraud Incident?

Fraud essentially involves using deception to make a personal gain for oneself dishonestly and/or create a loss for another. Although definitions of fraud vary, the incidents of _fraud' commonly include activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion.[1] Surveys are regularly carried out to estimate the true scale and magnitude (cost) of fraud to business and society. While findings vary, there is unanimity on the increasing prevalence of fraud within organizations and it (fraud) continues to remain a serious threat and a costly problem. Fraud incidents are increasing due to

[1] Corporate Fraud : Topic Gateway Serial No.57, Chartered Institute of Management Accountants, Street London SW1P 4NP United Kingdom (Page 3)

greater globalization, more competitive markets, rapid developments in technology and periods of economic difficulty. *However, for avoiding ambiguity and to be n sync with the regulatory (as per the latest RBI) directions on the incidents of fraud will be reckoned as basic determinants on a fraud incident.* To have uniformity in reporting, the RBI directs to classify frauds, mainly on the provisions of the Indian Penal Code, as under:

a. Misappropriation and criminal breach of trust;
b. Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property;
c. Unauthorized credit facilities extended for reward or for illegal gratification;
d. Cash shortages. e. Cheating and forgery; and
e. Fraudulent transactions involving foreign exchange.

4.2. Extent of Fraud Incidents: Global , National and at Organizational Levels

**4.2.1.** Association of Certified Fraud Examiners (ACFE) in their latest ―Report[2] to the Nations: 2018 Global Study on Occupational Fraud[3] and Abuse‖ has highlighted the following key findings on the extent of fraud :

a) That during the period under report (January,2016 to October,2017), 2690 fraud cases[4] were reported from 125 countries in 23 industry categories. Region-wise, United States constituted for 48% cases, SubSaharan Africa for 13% cases, Asia-Pacific for 10% cases, Western Europe for 6% cases, Latin America and the Caribbean for 5% cases, Middle East and North Africa for 5% cases, Southern Asia for 5% cases, Eastern Europe and Western/ Central Asia for 4% cases and Canada for 4% cases;
b) That the total loss amounted to $7billion with median loss per case of $130,000;
c) That corruption was the most common mode of occupational fraud in every global region;
d) That asset misappropriation are the common mode accounting for 89% of cases and financial statement frauds accounted for about 10% of cases;
e) That tips are the most common initial detection method (40% of cases) followed by internal audit (15% of cases) and management review (13% of cases);
f) That employees provided 50% of tips and nearly 33% of tips came from outside parties;
g) That organizations with hotlines detected fraud tips more often (i.e. 46% of cases) and non-hotlines cases were about 30% of cases;
h) That internal control weaknesses were responsible for about 50% of fraud cases;
i) That data monitoring / analysis and surprise audits were correlated with the largest reduction in fraud loss and duration; *and*
j) That only 4% of perpetrators had a prior fraud conviction history.

**4.2.2.** According to a report in ―Economic Times‖ dated 07th August, 2018 Indian banks reported a total loss of about Rs 70,000 crore due to frauds during the last three fiscals up to March 2018. The extent of loss in fraud cases reported by scheduled commercial banks (SCBs) for 2015-16, 2016-17 and 2017-18 was Rs 16,409 crore, Rs 16,652 crore and Rs 36,694 crore, respectively. Similarly, ―The Business Line‖ on 06th August,2018 reported that there has been a jump in the quantum of funds involved in banks and other financial institutions during the year 2017-18 and as per data submitted by the Reserve Bank of India (RBI) to the Central Government, the amount increased to Rs.32,048 crore in the last (2017-18) financial year against Rs.23,930 crore in FY 2016-17. For public sector banks, it had gone up significantly from Rs.19,529 crore to Rs.29,246 crore. Nationalized banks witnessed a steep increase in frauds. Contrary to it, the Private sector banks witnessed a decrease in the amount involved in frauds. A look into the last five years' data reveals that there has been a three-fold increase in public money that was lost. For instance, in 2013-14, the amount involved was Rs.10,170 crore, and the number of reported frauds were only 4,306. According to a report in ―The Quint‖ dated 18th February, 2018 in 2016-17, 3,870 cases of bank fraud cases were reported amounting to Rs 17, 750 crore across banks including commercial and private banks. The increase was most probably due to stringent investigations undertaken by banks on corporate and other advances. The Central Vigilance Commission (CVC) has analyzed 17 large-value accounts across seven different sectors including gem and jewellery, manufacturing/industry, agro, media, aviation, service/projects and discounting of cheques.

[2] The report contains an analysis of 2690 cases of occupational fraud that were investigated between January,2016 and October, 2017.

[3] *Occupational Fraud* is defined as the use of one's occupation for personal enrichment through deliberate misuse or misappropriation of the employing organization's resources or assets.

[4] Which the study reported to constitute only a tiny fraction of the frauds committed against organizations worldwide during the above period.

i. **4.2.3.** At organizational (J&K Bank) level, our bank has seen vulnerabilities of fraud incidents on both liabilities and assets portfolio . A perusal of the fraud incident of the three years (FY 2014-15, FY2015-16 and FY2016-17) indicates:

ii. That in all 56 fraud cases (12 in FY2014-15, 19 in 2015-16 and 25 in 2016-17) were detected and reported during last three years i.e. FY 2014-15 to FY2016-17 involving Rs.1226.96 crores with recovery of Rs.404.86 crores and net loss of Rs.822.10 crores. As against 25 fraud cases detected and reported in FY 2016-17, the number of fraud incidents detected and reported in FY 2015-16 and FY 2014-15 were 19 and 12 respectively indicating Y-o-Y increase of 06 cases in FY2016-17 and 07 cases in FY 2015-16;

iii. That thirteen large value (Rs.1.00 crore and above) cases were detected and reported during the above period involving Rs.1218.34 crores with recovery of Rs.401.16 crores and net loss of Rs.817.18 crores; iv. That most of the large value frauds (12 out of 13) have occurred in advances portfolio covering bills discounting (Rs. 221.04 crores); cash credit (Rs.15.89 crores) and term loans (Rs.980.42 crores);

v. The one large value fraud of Rs.1.00 crore has occurred in cheque collection/ clearing and the amount stands fully recovered;

vi. That most of the large value frauds 92.31% occurred in credit portfolio of the bank;

vii. That in **FY 2014-15 ,**out of twelve fraud cases, one fraud incident occurred in clearing of instruments, one in internet banking, one in inter-branch accounts; two in deposit accounts and seven in credit portfolio;

viii. That in FY 2015-16, nineteen fraud incidents were detected/ reported with 10 episodes in deposit portfolio (savings : 6; current : 2; term : 2), one in remittance-in-transit and seven in advances portfolio. The pattern of most of the frauds being perpetrated in deposit portfolio is in contrast to the segment-wise occurrence of frauds in advances portfolio in FY 2014-15. *Hence, it is seen that both deposits and advances portfolios carry similar fraud-risks;*

ix. That in FY 2016-17, out of 25 fraud episodes detected/ reported , 15 cases related to advances; 07 to deposits ; 02 to cheques/DDs and one in internet banking; and

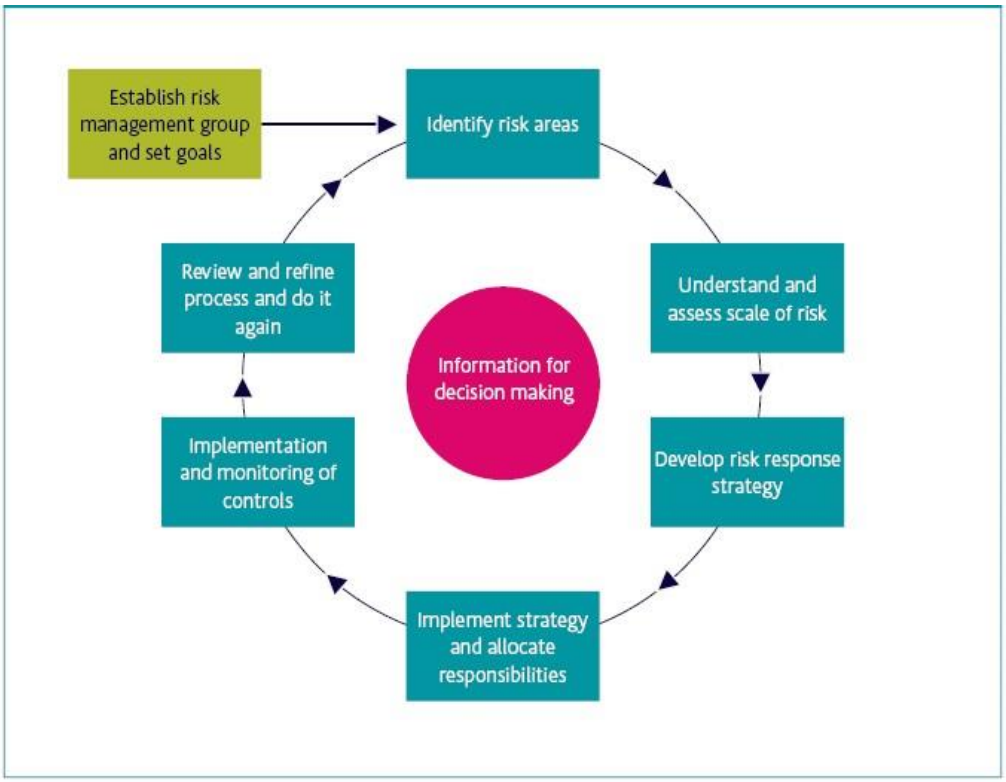
x. That the above trend of fraud cases detected/ reported during last three financial years reveals an irregular pattern wherein both deposits and advances portfolios are observed to be most vulnerable to fraud incidents with a few incidents in cheque clearing/collection and internet banking.

In the financial year 2017-18, in all 18 cases, entailing Rs. 215.12 crore were reported by the bank to the RBI as frauds including 12 credit related frauds and 6 non-credit related frauds. Upto 30.09.2018, the bank reported 04 (four) fraud cases involving Rs.120.98 crore including two credit-related frauds for Rs.120.68 crore. The snapshot of this data is given in annexure —A‖.

**5. Integrated Strategy for Prevention & Control of Frauds.**

5.1. Components of the Integrated Strategy for Prevention & Control of Frauds.

As fraud risks are real and growing continuously, so any strategy to address fraud vulnerabilities has to be comprehensive & dynamic to keep pace with the changing requirements of the bank. The six-generally accepted components of the risk strategy also applicable to fraud incidents are given in the Figure 1 below[5]:




5.2. Two Aspects of Identification of Fraud Risks. The current banking operations of the bank has **two main aspects** for identification of fraud risks:

**a) Online Frauds: Operationalization of the Transaction Monitoring Cell.**

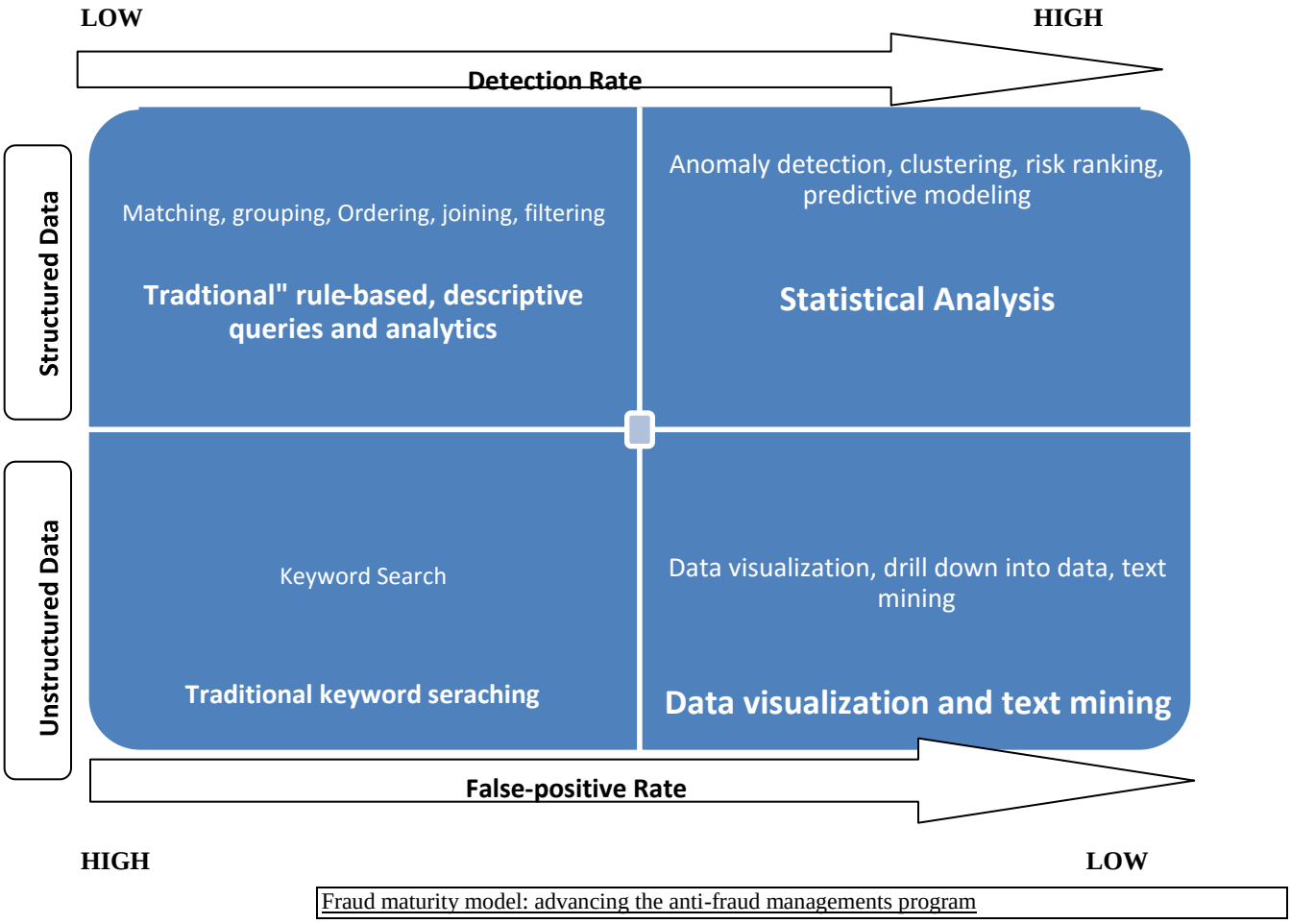
5.2.1 Online Frauds are posing a serious challenge to the banking operations as with the increasing use of technology and digitization, the fraud landscape has shifted to use of internet by rouge elements and their network across globe thereby making the use of existing boundaries and laws at times redundant and necessitating that an ―institution's operational (fraud risk) management must … be sound, meaning that it must be commensurate with the nature, size, risks and complexity of … (the) institution's activities.‖[6] The most effective fraud tools[7] commonly used for preventing online frauds are:

i) Address verification service;
ii) Card verification number; iii) Device fingerprinting; iv) Fraud Scoring Model;
v) Payer authentication (3-D Secure);
vi) Credit History Check; vii) Email Verification; viii) Customer Order History; ix) Negative Lists; and

[5] Adopted from ―Fraud Risk Management: A Guide to Good Practicel, Chartered Institute of Management Accountants 2008, Page 25.
[6] Good Practice Document on Integrity Risk Appetite : DeNederlandsche Bank , Eurosystems : Page 4
[7] Online Fraud Benchmark Report : Persistence is Critical , 2017 North America Edition, Cybersource : Page 6

x) Two-factor phone authentication.

To move forward in prevention, detection and deterrence of on-line frauds the bank has set up a Transaction Monitoring Cell (TMC) as per the latest regulatory guidelines of the RBI. *The bank is in the process of setting up an Enterprise-wide (online) Fraud Risk Management Solution (FRM) which is under negotiation for commercials at apex committee. It is hoped that the FRM for the TMC will be in place in a few months' period for monitoring online transactions of all business verticals including credit/ debit cards, SWIFT, CBS, mobile banking, Online banking etc.* The comparative use of traditional key-word searching and data vitalization and text mining vis-à-vis the structured data rule-based, descriptive queries and analytics as given in the table below shows high rate of anomaly detection, clustering of data and predictive modeling.




Fraud maturity model: advancing the anti-fraud managements program

5.2.2. Way Forward: Digitization of On-line Fraud Risk Management.

Fraud risk can be costly for banks. According to Oliver Wyman[8] net fraud losses often reduce a bank's operating income by 80 basis points (bps). Fraud risk can also have a negative impact on the customer experience, thus limiting business growth. So there is a broader business case for effective fraud risk management which can boost profitability in two ways. Firstly, by improved bottom-line performance from reduction of fraud related losses and lower operating costs by saving on staff expenses involved in fraud management. Secondly, there would be revenue growth through customer-centric approach to business. Hence digitization of bank's fraud risk management capabilities is very crucial and critical. Analogous to credit risk, a bank cannot do business without being exposed to fraud risks and

[8] Source: Oliver Wyman's proprietary fraud loss benchmarking data base.

losses. So there is need for a bank to decide the trade-off between business growth and the level of security. Though this dilemma cannot be completely resolved , yet the bank can enhance its fraud risk management capabilities in a way that makes higher growth possible without undermining security aspects. Digitization helps to increase efficiency and reduce costs. By making use of big data and machine learning for fraud monitoring, the bank would certainly minimize fraud related losses and costs. Besides, digitization would promote a seamless customer experience, bolstering potential for business growth.

The digitization of fraud risk management capabilities within the bank requires a combined effort across both the first and second lines of defence. Various functional areas like business, operations , technology/ data and risk management departments need to participate in active fraud risk management and decision making. This task is assigned to Fraud Risk Management Group (FRMG) of the bank (**see Para 5.5 at page 13**).

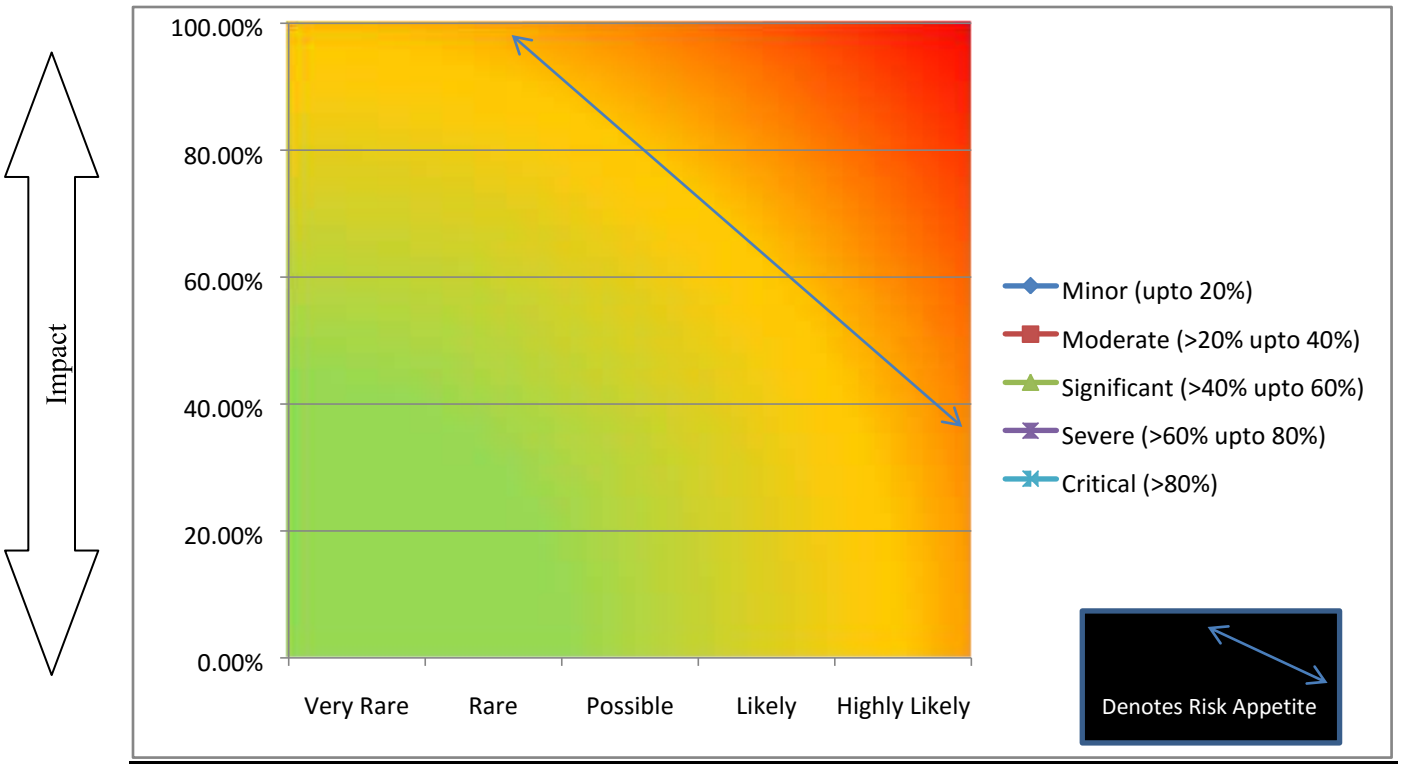
**b) <u>Vigilance Framework for Other Operational Areas.</u>**

For preventing frauds in other operational area of the bank, Vigilance Department besides going for revamping its functioning through a third party assessment (for which an EoI is underway) is planning to put in place bestpossible technology-driven solutions/ frameworks including use of artificial intelligence/Fraud Risk Solution for prevention and early detection of fraud incidents throughout the entire enterprise besides developing an MIS (Management Information System) for Vigilance Department for tracking the progress of various cases as per the stipulated TAT (Turnaround Time ) and for taking various actionables to their logical conclusion in an efficient, transparent and accountable way. Simultaneously policy framework, systems and procedures are re-visited to remove redundancies and for improving the efficacy of existing procedures for supporting the larger corporate/ business goals to meet the expectations of all stakeholders. For this purpose the present Preventive Vigilance Framework is devised and operationalized.

## 5.3. <u>Understanding & Assessing Scale of Fraud Risk</u>.

Historical data given at para 4.2.3clearly indicates that both liabilities and assets sides of the bank‘s balance sheet are subject to fraud incidents. Hence for understanding and assessing the scale of fraud risks in both deposits and advances in addition to other related operational areas, all business unit /operational areas would be required to make periodical assessment of their vulnerable areas**. <u>*At macro level, the bank would be taking periodic*</u> <u>*assessment through specialists in the industry for assessing the efficacy of the extant systems & procedures so*</u> <u>*that the fraud vulnerable areas are identified and suitable steps initiated for taking the fraud-prevention and*</u> <u>*detection measures to next level of compliance with timely action*</u>**. The fraud risk assessment exercise would be taken for all areas and processes of the business in terms of impact and likelihood. In addition to the monetary impact, the assessment would consider non-financial factors such as loss to reputation and brand-image of the bank. The assessment would also be required to give inputs on likely /emerging fraud risk areas and the measures needed to strengthen fraud prevention and detection mechanism of the bank so that the fraud preventive framework would continue to evolve in line with the emerging challenges from fresh fraud vulnerable areas. This will be in addition to the in-house feed-backs from inspectors/ auditors and staff from time to time under different compliance measures already in vogue.

However, for the time-being the assessment would be made by the business unit/ other operational levels on the basis of the fraud preventive measures (see table/s at Para 6) . For quick visualization of main fraud areas in a business-unit/ zone, the table below would be used to represent aggregate of individual fraud-risks of branches fraud assessments. As the fraud-risk areas will substantially vary from one business unit to another in view of different business profiles and other (e.g. external) factors impacting the incidence of frauds, so each business unit would be advised to use its own check-list out of the overall table given at Para 6 of the ―framework‖.




**Likelihood of Occurrence**

5.4. **Developing Fraud Risk Response.**

The bank's approach to dealing with fraud incidents is clearly elaborated in the **"Policy Framework on Fraud Risk Management & Vigilance (2017-18 version)"** which is subject to review & revision from time to time in view of statutory guidelines and other fraud risk measures based on business dynamics that the bank would take for prevention, detection, reporting and recovery. *The Fraud Risk Plan (FRP)* is now intended to further improve the extant procedures which allow for evidence gathering and collation. The FRP of the bank would include/ focus on the following aspects:

5.4.1. Purpose of the Fraud Response Plan .

The main aim of the FRP is to take suitable steps for responding to a suspected or detected fraud incident by:

(i) a clear reporting mechanism,
(ii) conducting a thorough investigation into the incident of fraud (suspected or detected),
(iii) taking swift and speedy action for disciplining the individual responsible (internal, external, civil and/or criminal),
(iv) effective measures for recovery of fraud-impacted funds and/ or assets, and
(v) modification in the extant systems & procedures / anti-fraud strategy to prevent recurrence of similar incidents/ events in future.

All these aspects are clearly detailed in latest **—Policy Framework on Fraud Risk Management & Vigilance ( 2017-18 Version) available on the internet of the bank,** which would be further strengthened by this framework document for reiterating the bank's commitment to high professional, legal, ethical and moral standards in all its activities, and its approach in dealing with/ attending to the deficient areas. The fraud risk response would be a cross-section responsibility and would be looked after by —Fraud Risk Management Group‖ of the bank. *However, for on-line banking operations (which is more vulnerable to frauds with use of internet and other applications for increasing digitization of banking operations as the banking transactions are moving from land to skies), the TMC with the help of T&IS/ other Departments would be advised to prepare proper / welldocumented policy framework*

*for mitigating cyber/ online frauds with a proper Fraud Risk Plan involving all stakeholders so that any on-line fraud incident is attended to with utmost urgency and with a speedy, swift & appropriate response.* **However, for the time being the job of mitigation and monitoring of online/ cyber frauds will be assigned to the FRMG as given at para 5.5. below.**

5.5. **Re-constitution of Fraud Risk Management Group.** As vulnerability of frauds in possible on both liabilities and assets side of the balance sheet of the bank so for addressing various issues related to it, an integrated strategy is needed wherein all concerned departments of the bank from Corporate Headquarters would be involved in contributing to mitigation of various fraud risks and flagging the concerns arising out of various fraud vulnerabilities of the bank in a timely manner**. Hence, it is proposed that we may reconstitute the Fraud Risk Management Group with following members:**

i) President / Vice President (Vigilance) ; Overall incharge of the FRMG; ii) Vice President (IRMD)/ Chief Risk Officer: for associating him with fraud risk assessment and Fraud Risk Appetite of the bank ;

iii) Chief Internal Security Officer (CISO) : for information security issues;

iv) Vice President (S&C) : for issues related to strengthening the extant systems & procedures/ plugging loopholes/ reviewing efficacy of various internal audits/ inspections ; and

v) In-charges of Vigilance/TMC/T&ISD/ Data Centre/Payment & Settlement/MIS Departments : for issues related to their respective departments.

**Besides, representation will be sought from other stakeholders related to different aspects of fraud-risks as given in the table below from time-to-time as per the urgencies/ needs and requirements of the case/ situations under consideration/ discussion:**

| Fraud Risk Category | Ownership with Departmental Heads |
|---|---|
| Compliance Issues | Chief Compliance Officer (CCO) of the bank |
| Isolating staff with Corrupt tendencies and/ or having record of corrupt-practices from sensitive positions/ posts and maintenance of their proper record. | Topmost Officer in the management hierarchy looking after HRD i.e. presently we have Executive President (T). |
| Loss to Physical Assets and Security | President (S&IT)/ Vice President (Estates)/ Security Officer |
| Financial Reporting | Chief Financial Officer (CFO) of the bank |
| Anti-trust/Legal Issues | President, Law Department, CHQ |
| Periodic Assessment of ―life style‖ of staff and maintenance of records thereof. | Zonal Heads within their respective areas and Vice President (HRD, CHQ) for staff posted in Zonal Office/ Corporate Headquarters. |

## 6. Implementing Fraud Prevention Strategy & Allocation of Responsibilities for Establishing a Fraud Control Environment in the Bank.

6.1. Establishing a Fraud Control Environment: Beginning Steps. To begin with, for establishing a Fraud Control Environment (FCE) for prevention of fraud incidents and allocation of responsibilities, the following are some of the measures assigned to various levels to pursue/ follow these proactively:

| Areas of Fraud | Preventive Measures | Action-point assigned to |
|---|---|---|
| 1. Misappropriation and Criminal Breach of Trust | • Persons of doubtful integrity not to be posted in sensitive posts.<br>• Regular scrutiny of staff accounts by Branch Manager at Branches and Branch Manager's account to be scrutinized by Zonal Managers.<br>• Branch Manager to examine exception report daily which is generated at EOD without fail. | i)HRDD, CHQ<br><br>ii)Concerned Branch / Zonal Heads<br><br>iii)Branch Head |

| | | |
|---|---|---|
| 2.(a) Illegal/Irregular manipulation of records, documents, withdrawal of money etc. | • Cross-checking of transactions by staff other than the one effecting the transaction initially. • Bank is having policy in place on User Id and password. | i)As per the best practices currently in vogue in the banking industry, the Branch Head and other staff members not to leave the branch |
| | • Careful and continuous monitoring of the work done in sensitive areas particularly deposits and advances. | premises without cross-checking of vouchers (both credit & debit) each day. Cross-checking as per the practice, implies that voucher with the system will be checked by third person (other than maker-checker). In case of small branches, it will be done exclusively by the business unit head before submitting sol/ completion of day-end process. This will prove a great deterrent against internal frauds. ii) Concurrent Auditors to report its compliance in their monthly reports : S&C, CHQ |
| 2.(b) Forgery of documents/vouchers/records | i) Keeping under safe custody to avoid fraudulent manipulations. ii) Loan documents taken ought to be vetted by Bank's lawyers- more so in case of equitable mortgage. iii) Inspecting officers to cross check at random, particular records relating to large value transactions | i)Record Keeper/ daftari under the supervision of Hall-incharge/ Branch Head for daily transaction including vouchers ii) Joint responsibility of Manager Advances & Branch Heads with legal counsels/ Zonal Law Heads as per extant guidelines on the subject from A&AP CHQ/ Law Department, CHQ iii) Both current and RBIA auditors as per their respective periodicity. |
| 2(c) Falsification of loan documents : Internal Fraud Elements | i) Reinforcements of instructions emanating from controlling office/s regarding execution of documents and the same have to be put into practice. Instructions are to be carried out within laid down time frame and deviation must be followed up with appropriate action. ii) Balancing of GL heads of non-fund based credit limits with their respective subsidiaryGL heads in the CBS environment is a must. A printout to be taken out from the system and to be checked and verified. | i)To prevent internal frauds & impersonlization of loan documents with the collusion of staff having malicious motives, it shall be joint responsibility of both Manager Advances and Branch Heads to get the documents signed in their presence and certify the same in each borrowal account. ii) To ensure that the non-fund based credit facilities are extended / allowed as per the extant rules , Manager Advances would be solely responsible in extraction of reports of these heads from GL and tally with the records. iii) Issuance of BG‘s to be made system-driven in line with the ILC/ LC so that possibility of issuance of BG‘s outside the finacle / branch records is completely arrested . **(Action-point for A&AP , CHQ and Information Security/ T&ISD, CHQ**. |

| | | |
|---|---|---|
| 2(d) Fraudulent encashment through forged instrument colored Xeroxed/ scanned cheques | • Check MICR code/ISFC code printed on the cheque for its correctness.<br>• Scrutinize quality of the printing/ paper which is inferior before making payment.<br>• Scrutinize carefully to detect any change *in* the colour on the face/back of the cheque presented for payment.<br>• All high value cheques received in inward clearing/ speed clearing/ payment must be | Laxity of staff assigned the job of posting/ passing of cheques , has been one of the prominent features in payment of forged/ fraudulent instruments . Proper due diligence by the operational staff associated in posting/ passing of cheques is required. As payment against a forged/ fraudulent instrument in |
| | checked by Ultra Violet Lamp before making payment as per the RBI guidelines.<br>• In case of any doubt, immediately contract the issuing branch/ customer to verify the genuineness of the instruments & instructions. | —NOT PAYMENT IN DUE COURSE AS PER THE NEGOITABLE INSTRUMETNS ACT AND COURT DECISIONS ON THE SUBJECT‖ so staff are advised to remain careful and vigilance in making payment against forged/ fraud instruments .<br>PREVENTION OF PAYMENT AGAINST A FRAUD / FORGED INSTRUMENT IS THE ONLY REMEDY. |

| | | |
|---|---|---|
| 2(e) Forgery in Demand Drafts and Issuance of Fake Drafts | i)All Demand Draft leaves should invariably be kept under proper custody and use of the same must be accounted for each day. ii)At the time of making payment, each Draft leaf must be examined carefully to notice that it has: • Printed number containing specified digits.<br>• The correct Code Number of our Bank and Draft Transaction Number.<br>• Water mark is present on the Draft leaf in the form of our Bank's logo, which should be visible if hold against light.<br>• Name of issuing Branch with correct Code No. is mentioned on the Draft.<br>• Correct name and Code No. of the branch on which the Demand Draft is drawn has to be checked.<br>• The texture/paper quality of computer generated Draft leaf has to be examined to ascertain its genuineness.<br>• Colour of the Draft must be identical with that of the genuine Draft of our Bank.<br>• The signatures appearing on the Demand<br>Draft must be carefully verified from the Specimen Signature Book available with the branches before payment made for the Demand Drafts. Greatest attention should be given to the identification number of the signatories on the Draft.<br>• When instance of fake/ forged draft comes to notice, the incident is circulated among all branches/ offices to exercise caution for obviating recurrence of such incidence. • Master List of all previous notified stolen/fake security documents to be maintained at branch level.<br>• There should not be any material alteration in the amount written both in words and figures in the Demand Draft. | i) Manager accounts of each business unit.<br><br>ii)Joint responsibility of the makerchecker in each transaction. |
| 2(f) Dividend Warrants/Interest Warrants/ Refund Payment | • Reference should always be made to the circulars issued regarding payment of<br>Dividend Warrants. If a particular branch is not designated as the Paying Branch, but the Dividend Warrant is presented for payment, the same should be declined and the matter referred to the controlling office.<br>• The colour of the instrument presented for payment must be carefully compared, whenever necessary, with the specimen of the instrument circulated among branches | Joint responsibility of the makerchecker in each transaction. |

| | | |
|---|---|---|
| | designated for payment.<br>• The instrument itself should be carefully scrutinized to find out whether the number mentioned therein tallies with the number as communicated through circulars for payment of Dividend Warrants. Special attention should be given to the Control Number of such instruments.<br>• Sometimes the upper limits of the amount are fixed for payment of Dividend Warrants and hence, while making payments, it should be ensured that the warrant being paid is not of an amount exceeding the limit.<br>• The signatures on the Dividend Warrants must be carefully compared with the signatures circulated among the Paying Branches and it should be ensured that no Dividend Warrant with a different signature is paid. | |
| 2(g) Acceptance of National Savings Certificates as security | • At the time of accepting National Saving Certificate (NSC) as securities for disbursing credit facilities, the following aspects are to be carefully examined.<br>• The NSC to be examined carefully to ensure that it is genuine and not a spurious one.<br>• There should not be any overwriting/cancellation without authentication.<br>• NSC should be sent to the Issuing Post Office for Registration and lien marking.<br>• In no case the NSC should be handed over to the prospective borrower for getting lien marked/ pledged by the concerned Post Office, but some authorized persons from the Branch should approach the Post Office for this purpose.<br>• While effecting encashment of NSC for adjustment of loan, the same should be sent to Post Office through an authorized person of the Branch and payment obtained directly.<br>• NSCs offered as security are to be kept always under proper custody and no unauthorized access be allowed to the same. | Joint responsibility of Manager Advances and Branch Head. |

| | | |
|---|---|---|
| 3)Unauthorized credit facilities extended for reward or for illegal gratification | • Inspection reports raised on branches must be meaningfully analyzed at controlling offices and any lacunae pointed out therein should be taken up with the concerned branch for removal of such shortcoming infirmities within the definite time frame.<br>• Controlling offices must monitor and analyze various statements sent to them relating to credits disbursed and deviations noticed are to be rectified within reasonable time, keeping close watch on the procedures undertaken for rectification. | i) Joint responsibility of Manager Advances and Branch Head for extending only legal/ genuine credit facilities as the policies & procedures circulated by the bank from time to time.<br>ii) Monitoring the efficacy of the System : Respective Credit Monitoring Departments at Cluster/ Zonal / Corporate Headquarters level.<br>iii) Respective S&C Division with S&C, CHQ to seek inputs from concerned Credit Monitoring Departments of the Cluster/ Zone and Concurrent –RBIA auditors as per the periodicity of their respective audits. |

| | | |
|---|---|---|
| 4) Negligence & Cash Shortages | • Cash Keys are to be kept under dual custody. Movement of keys to be properly recorded. • Cash safes to be operated always by both custodians together.<br>• No unauthorized persons to be allowed in cash strong room and cash department enclosures.<br>• Physical verification of cash to be invariably undertaken each day after the close of business hours. | Joint responsibility of the concerned Cashier and the Manager Accounts. |

| | | |
|---|---|---|
| 5(a) Cheating and Forgery (a) Fake Title Deeds in Mortgage Loan | • Strict adherence to Bank's guidelines/ policies/ systems & procedure in this regard. • Due diligence on builder/ seller/ borrower<br>• Due diligence of property independent of borrowers/ lawyer by both Manager Advances & Branch Head.<br>• Title Deeds are to be verified carefully so as to prima facie establish the genuineness of the same.<br>• "No Objection" Certificate and other documents issued by builders and housing societies must be carefully examined about their genuineness.<br>• Pre & Post Sanction verification by two different officers.<br>• Sites of properties offered as securities must be visited to ensure its existence before loans are sanctioned/ disbursed.<br>• Valuation of the property offered as security must be conducted by Registered/Empanelled valuers.<br>• Valuation by officers independent of valuer also to be done.<br>• It has to be ensured that the Title Deeds offered as security for a particular credit facility availed is free from encumbrance. • Search certificate for minimum twelve years should be obtained from the empaneled Advocate of the Bank. The date of the certificate should tally with the actual date on which the search was conducted from Search Receipt.<br>• Certified copy of the title deed should be obtained from the Sub Registrar's office and compared with the original one submitted by the borrower as per Circulars.<br>• Valuation report must be obtained as per latest format and guidelines of the bank issued under Circulars.<br>• An independent valuation must be done by the branch officials to rule out overvaluation, | Joint responsibility of Manager Advances and Branch Head. |
| 5(b) Impersonation | • The principle of 'Know Your Customer must be followed carefully<br>• Identification of individual/corporate entity opening an account so as to establish true identify/bona fides.<br>• Establishing identity of the customer by verifying passport, driving license etc. for individuals and Memorandum of Association, Articles of Association etc. for corporate bodies.<br>• Proper introduction of the account. | Joint & several responsibility of Manager Accounts/ Manager Advances and Branch Head for their respective-interconnected functional roles. |

| | | |
|---|---|---|
| | • Verifying information given by the customer himself.<br>• New account-holders are sent letters of thanks by Post for opening accounts & requesting them to bring the envelope to Bank<br>• Monitoring high value remittance<br>• Remittances of amount of Rs. 50,000/- and above to be made by debit to customer's accounts or against cheques and not against each.<br>• Applicants for remitting amount exceeding Rs. 10,000/- may provide PAN (IncomeTax). | |
| 5(c) Unusual activities/ transactions | • Proper monitoring of transactions are to be carefully undertaken in the following cases:<br>• Frequent, large cash transactions.<br>• Multiple accounts being operated under the same name<br>• Frequent conversion of large amounts of currency from small to large denomination notes.<br>• Placing funds in term deposits and using them as security for more loans.<br>• Large deposits immediately made following wire transfers.<br>• Sudden surge in activity level.<br>• Same funds being moved repeatedly among several accounts.<br>• Multiple deposits of money orders. Banker's cheques, drafts of third party.<br>• Transactions inconsistent with the purpose of the account.<br>• Low or overdrawn balance with high activity. | Joint & several responsibilities of Manager Accounts and Branch Head for their respectiveinterconnected functional roles. |
| 5(d) Fake Bank Guarantee | i) Issuing branch to send a copy of BG to the beneficiary requesting him to check up the terms and conditions of the bank guarantee.<br>ii)Branch to send their confirmation to the controlling office which shall exercise proper control against fraudulent issuance of the BGs.<br>iii)BG‘s to be issued must be system-driven on the lines of ILC/LC. | (i) & (ii) Joint & several responsibility of Manager Advances and Branch Head for their respective-interconnected functional roles.<br><br>iii) Issuance of BG‘s to be made system-driven in line with the ILC/ LC so that possibility of issuance of BG‘s outside the Finacle / branch records is completely arrested . **(Action-point for A&AP , CHQ and Information Security/ T&ISD, CHQ**. as given at 2 (c ) (iii) above. |

| | | |
|---|---|---|
| 5(e) False letter of credit submission | • Confirmation to be called for from issuing Bank immediately on submission of Letter of Credit by the party.<br>• Thorough scrutiny of the letter of credit to detect any onerous clause.<br>• Evaluating the terms/conditions to verify their practical enforceability or otherwise.<br>• L.C not to be opened for those who do not enjoy credit facilities without proper sanctions and justifications.<br>• The customers' ability to retire bills under L/C has to be considered and ensured. | Joint & several responsibilities of Manager Advances and Branch Head for their respectiveinterconnected functional roles. |
| 6) Delay in flagging the borrowal accounts as ―Red Flag Accounts‖ as per the RBI directions and delay in | Red Flag Signals to be observed/ watched/ analyzed by A&AP Division Corporate Headquarters as per the extant RBI guidelines | Vice Presidents and President/s A&AP to monitor it in their respective/ assigned areas. |
| attending to ―fraud alerts/ signals‖ thereby allowing the fraudsters to perpetrate fraud/s owing to delayed action/ inaction . | so that fraud alerts/ signals are attended to comprehensively for preventing possible losses to the bank owing to delayed action or inaction. | |
| 7) Cheque cloning | The contents and texture of each instrument as per the threshold limits of the RBI to be examined so that presentation of cloned cheques is arrested. | Business Unit Heads and RCC‘s as per the extant guidelines of the bank/ RBI on the subject. |
| 8) Mitigating People / Staff Risk in frauds | Besides, proper background checks as per the best-industry practices, the proper people / staff at proper places so that there is total synchronization in skill-levels and job-roles of the staff . | HRDD to create proper profiles of all staff/ people in the bank so that there is minimum due diligence in assigning jobs/ tasks/ roles suitability of each staff member is ensured. |
| 9) Gaps in understanding and using technology for banking operations and other administrative functions & roles. | The gap between ―old generation‖ staff (―digital immigrants‖) and new generation technology –savvy (―digital natives‖) for bridging the knowledge-gap between the supervisor and the supervised leading to loose controls in operations and controls. | HRDD to provides suitable training for bridging the knowledge gap between the old and new generation staff in the bank so that the areas of disconnect in the system are addressed/ attended to suitably. |
| | | |

## A) Preventive Measures for On-line/ Technology–Related Operations.

As the 21st Century has witnessed tremendous change in the mode people conduct their banking transaction with computerization and digitization of large volume of every-day transactions , so there is need for taking timely precautionary measures to minimize the related fraud risks. To address these issues, the following general preventive and curative measures are proposed :

| **6) Method of Computer Frauds/ Crime** | **Activity** | **Preventive Vigilance** | **Assigned to** |
|---|---|---|---|
| Data Diddling | Changing the input or output unauthorizedly to conceal or give erroneous output affecting the data integrity | Assigning proper users IDs/authentication | Joint responsibility of the SICO with In-charges of T&IDS/ TMC/ Finacle |

| | | | |
|---|---|---|---|
| Trojan Horse | Unauthorized but innocent looking instructions imbedded to the programs to activate and destroy data at a predetermined date. | Source code review of outputs - to data analysis | Team/ Other related departments. |
| Salami Technique | Theft of small amounts not drawing attention of authority in a big way. | End value/abnormal value null value analysis | |
| Super Zapping | Data over-write or erasing the data base through a program without leaving trace | Physical and logical access controls to be invoked. | |
| Trap Doors | Undocumented entry pontes in the programs switching over to activities not intended to under the prescribed rules | Program review and computer audit | |
| Scavenging | Left over information or unattended floppies or unused floppies having sensitive information used for | Unused information to be shredded/unused floppies to be erased before reuse | |
| | fraudulent activities | | |
| Data Leakage | Disclosing the information through covert means | Strong data safety methodsaccess controls | |
| Simulation and modeling | Using a back-up computer for entering fictitious records | Strong back – up procedures and door mented off-site backup procedures to be ensured. | |

While CBS has offered a host of convenient services for customers, it has also opened floodgates for unscrupulous activities. Bank is having well laid down CBS policy to take care of needs of the maintenance and safety of the system.

| **7) Other Online Areas of Fraud** | **Preventive/Curative Measures** | **Assigned to** |
|---|---|---|
| Stealing/Sharing of Password | Comprehensive guidelines in place on maintenance of password | T&IS Department may suggest further practicable stringent measures for preventing stealing/ sharing of passwords as the existing ones are foolproof. |
| Manipulation in any intermediary/ parking accounts | These accounts have to be monitored on daily basis. | MIS Department and Compliance Departments at Zonal levels to jointly monitor it. |
| Dormant Accounts | Inter branch transactions should not be allowed. | Branch Heads at operational levels in view of possibility of higher levels of frauds in this area. |
| Unusual transaction | Exception report to be checked on daily basis. | Branch Heads at operational levels. |

| | | |
|---|---|---|
| General Ledger | Cash Book/GL should be generated on day to day basis and it should be checked on daily basis. | Manager Accounts and Hallincharge. |

**B) <u>Money-Laundering : Extant Regulatory Guidelines for Preventing/ Detecting Frauds.</u>**

To avoid frauds relating to ATM, Internet Banking, Mobile Banking foreign transaction or any other co-related aspect of money laundering , the RBI has also directed to take following steps :

| **Areas of Fraud** | **Preventive/Curative Measures** | **Action-point assigned to[9]** |
|---|---|---|
| **8) Money Laundering** | a) Keeping close watch on cash withdrawals and deposits for Rs. 10 lacs and above in deposit, cash credit or overdraft accounts, and keeping record of details of such large cash transactions separately.<br>b) Effectively monitoring Corporate Accounts where deposits or withdrawals are primarily in cash rather than cheques.<br>c) Examining remittances in Corporate Accounts received from/made to sources apparently unconnected with the corporate/business activity.<br>d) Checking transaction with large volume credits through DD/TT/PO whereas nature of business does not justify such credits.<br>e) Finding out reason for single substantial cash deposit composed of many high denomination | Joint responsibility of Manager Accounts & Branch Heads of Business units. |

[9] Most of these steps/ measures are already in vogue.

| | | |
|---|---|---|
| | notes.<br>f) Reasoning out as to why frequent exchange of small denomination notes for large denomination notes and vice versa take place.<br>g) Reasoning behind retail deposit of many cheques but rare withdrawals for daily operations.<br>h) Keeping close watch and guard against several cash deposits/withdrawals, below a specified level, made by customers intentionally splitting the transactions into smaller amounts for the purpose of avoiding detection of transactions with high limit.<br>i) Preventing/controlling unusual activities of customers, such as, those who visit safe deposit areas immediately before cash deposits, depositing large amount of currency bearing indication that the amount has been brought from other banks, funds coming from countries/centers which are known for money laundering.<br>j) Account need not be opened for customers/company who are reluctant to provide complete information regarding purpose of opening the account.<br>k) Carefully monitoring those accounts of customers who have no record of past or present employment, but made frequent large transactions. | |
| **9)(**i)ATM/Debit Card related Frauds | Proper policy is in place for handling/ issuance/ activation of ATM/Debit cards.<br>Dual Control over ATM cash refilling, etc.<br>Reconciliation of cash in ATM with the balance shown in GL. | CISO, CHQ |
| 9(ii) Internet Banking/ Mobile Banking related frauds | Proper policy/guidelines are in place as per RBI guidelines .<br>Customers are also sensitized by the bank with regard to security threat to their internet banking transactions.<br>Password/PIN is issued to the customers directly on authentication. | CISO, CHQ |
| 9) (iii) Irregularities in foreign exchange transactions | a) Strict enforceability/observance of RBI guidelines related to such transactions.<br>b) Establishing, in foolproof manner, the credentials of the prospective customer before embarking on banking transaction with him.<br>c) Judicious approach to be undertaken while dealing with such matters. | President (CCB)/ President (CB) |

### C) <u>Preventive Measures for Curbing Frauds by Customers.</u>

Most of the frauds are nowadays committed by the outsiders and remain untraceable. To prevent the perpetrators from causing frauds the following preventive measures (which are only illustrative[10]) need to be meticulously followed-up for containment of frauds by customers:

[10] Further details / information can be obtained from different circulars of the Vigilance Department from time to time especially the ones on modus-operandi, which are available on bank's intranet.

| **10) Frauds by Customers/ Borrowers** | **Preventive/Curative Measures Already Existing/ Suggested** | **Action-point assigned to** |
|---|---|---|
| i) Open Account in fictitious name | | |
| a) With the help of introduction from existing account holder | a) The introducer must be well known to the Bank and his account must be operated satisfactorily for quite some time of at least six months. | Operational areas : Manager Accounts & his concerned staff |
| b) Taking advantage of negligence of Bank employees | b) Employees should be put on guard and whenever negligence comes to notice of authorities, immediate steps must be taken to obliterate the same. | Operational areas : Manager Accounts & his concerned staff |
| c) Persuading authorities by narrating false stories of the immediate need of opening account | c) "Know your customer" principle must be observed. Unknown persons are not to be accommodated howsoever rosy picture they may give about their selves.<br>d) photographs/identification documents must be taken for establishing identity and must be verified with the original.<br>e) Thanks letter to be sent to introducer and depositor at the given address to confirm the genuineness of the address of depositor. | Operational areas : Manager Accounts & his concerned staff |
| ii) Acquire cheque books, bank drafts through forgery/misrepresentation and tamper with cheques/drafts by fraudulently altering date, name of the payee and amount | ii) Cheque books[11] to be issued only to the account holder. Drafts to be delivered only to the person requisitioning the same or to authorized persons. Great care need to be taken while making payments for cheques/drafts. The signatures appearing thereon are to be carefully compared with specimen recorded. Instruments are to be carefully scrutinized to obviate chances of interpolation in drafts and cheques. | Operational areas : Manager Accounts & his concerned staff |
| (iii)(a)Undertake immediate high value operation and subsequent closure of account | iii)(a) Forged/ill-gotten cheques are deposited as "one time" operation and in such cases steps are to be taken to apprehend the culprit, which is possible only when the Bank is aware of the status of the customer. | Operational areas : Manager Accounts & his concerned staff |
| b) Confidence of Bank employees is won over initially by few genuine transactions and then forged cheques/drafts are deposited and whole amount withdrawn | b) Past transactions are to be carefully examined to find out the trend and see whether a single large transaction is compatible with past records. Any suspicion arising must be thoroughly investigated before further operation in the account is allowed. | Operational areas : Manager Accounts & his concerned staff |

[11] To be issued only to the account-holder in person and not to his authorized person as per the latest CHQ instructions.

| | | |
|---|---|---|
| iv) Sometimes Bills of Exchange supported by false transport receipts are discounted at the Bank, but goods not sent at all.<br>When discounting Bank sends the MTR to its destination with the Bill, the same is returned and Bank loses the money already given. | iv) Such bill discounting facilities are to be allowed to parties with established credentials and MTRs of reputed operators approved by IBA are to be accepted. Even when transport companies hand over goods to drawee of the bill without Bank's authority, the mater should be immediately taken up to receive the full value of the bill. | Manager Advances jointly with the Branch Head |
| v) Unscrupulous traders, businessmen obtain undue credit facilities against hypothecation of useless goods which are not of the desired quality and/or quantity. | v) This has to be avoided by undertaking regular and adequate inspection/supervision of the stocks by branch officials at irregular intervals. | Manager Advances jointly with the Branch Head |
| vi) Fake Title Deeds are submitted cleverly or impersonation resorted to as land/building owners while offering the same for equitable mortgage as collateral security. | vi) (a) Such Title Deeds must be scrutinized thoroughly to find out the veracity. Even spot verification by authorized persons have to be undertaken as a rule without exception. Established registered valuers with impeccable records are to be engaged for evaluating the properties. Non-encumbrance certificates have to be obtained from Registrar's office/Court without fail.<br>(b) Certified Copy of the title deed is to be obtained from the registrar and the title deed submitted by the client is to be verified to ascertain its genuineness. (c) Collateral security from third party should normally be avoided. | Manager Advances jointly with the Branch Head |
| vii) Unscrupulous persons promise to bring in huge deposits (particularly fixed deposits) with the condition that they would be allowed credit facilities (at lower rate of interest) against those deposits in their name although the deposits are kept in the Bank in some other persons names | vii) When accepting such deposits, care should be exercised that such deposits are genuine and all KYC norms have been fulfilled. | Manager Accounts/ Manager Advances jointly with the Branch Head |

### D) <u>Preventive Measures for Curbing Frauds by Bunko (Swindler) Banker.</u>

Beyond this, the possibility of banking frauds is also very high if the bank employee himself, who knows all the technicalities, operational strategies, flaws, and has access to all the relevant confidential information which is useful for banking institutions. This knowledge of his may prove immensely harmful, if disclosed to create any scam or any other forms of misappropriation of funds . Some of the precautions to prevent insider frauds (by employee) as follows:

| **11) Frauds by Bank Employees** | **Preventive/Curative Measures Already Existing/Suggested** | **<u>Action-point assigned to</u>** |
|---|---|---|

| | | |
|---|---|---|
| a) Banking Industry is vulnerable to insider abuse. It is often the most trusted employees who perpetrate the greatest fraud. | a)<br>i) Rotating employees' work assignments at intervals,<br>ii) Concept of maker and checker under CBS-Ensuring two or more persons are involved in one transaction,<br>iii) Implementing independent internal and external audit programs,<br>iv) Employees should be encouraged to take leave for at least fifteen days per year. | i)Business Unit Heads<br>ii) Business Unit Heads<br>iii) Efficacy of the existing audits and inspections to be strengthened : S&C, CHQ iv) HRDD. |
| b) Huge amount of cash in branch unnecessarily giving scope of surreptitious removal of cash | b) Minimum amount of cash depending upon the daily average requirement must be kept at the branch as per the extent guidelines. | Business Unit Heads |
| c) Inward "clearing" cheques coming to branch for debit of an account are quietly destroyed and not entered in the account. Excess balance in the account because of non-debit of the cheque is withdrawn soon after. | c) Usually these fraudulent transactions take place through clearing suspense account. Hence, clearing suspense accounts of the branch are to be checked daily and closely monitored. | Business Unit Heads |
| d) Customers are persuaded to keep their fixed deposit receipts with Bank after discharge and then the same are utilized by the staff for taking loan in his name. | d) i) Fixed deposit receipts must be kept under proper security and if any loan is obtained by the customer there-against, proper lien marking has to be made on the receipt itself as well as on relative books. ii) Advance in-charge of the branch has to verify the identity of the depositor before sanctioning and disbursing the loan. | Manager Advances and Business Unit Head |
| e) Unauthorized handling of transactions in dormant accountsaffording false/fake credit and subsequently withdrawal from the accounts | e) i) Dormant/inoperative accounts-Any operation thereon must be authorized by Branch Head as per the extant guidelines .<br>ii) During operation in such accounts, the Bank must obtain satisfactory proof that the transaction is taking place as per the mandate of the real account holder. | Manager Accounts & Head |
| f) Tampering with pass books of customers, which have been left with Bank's staff for updating and then surreptitiously withdrawing amount from the account | f) i) Close supervision be maintained for updating of passbooks left behind or long periods,<br>ii) Special care to be taken in those cases where transactions are not frequent. | Hall-incharge/ Manager Accounts concerned with staff. |
| g) Tampering with Specimen Signature Card to interpolate fictitious/ wrong names to show as operators | g) Access to such cards to be restricted to authorized persons only. If any doubt arises, the account holder(s) must be called upon to explain. | Hall-incharge/ Manager Accounts concerned with staff. |

| | | |
|---|---|---|
| h) Vouchers are tampered with and/or removed to suppress fraud committed | h) i) Register for voucher must be checked daily by an authorized officer.<br>ii) Number in register must tally with total number entered in printed DAY BOOK.<br>iii) Vouchers must be stitched and sealed properly date-wise everyday and kept under authorized custody. | Hall-incharge/ Manager Accounts concerned with staff. |
| i) Fictitious credits are offered in accounts and money withdrawn fraudulently. In order to suppress such transactions, manipulations are made in balancing of books. | i) Proper balancing of books and crosschecking of supplementaries are to be undertaken without fail. Deviations noticed must be rectified immediately. | Hall-incharge/ Manager Accounts concerned with staff. |

### E) Preventive Measures for Curbing Frauds by Customers/ Borrowers/ Outsiders in Connivance with Bank Staff.

Connivance of bank employee with outsider invariably further increases the possibility of committing banking fraud. Following preventive steps to address the frauds by staff in connivance with outsiders are needed:

| **12) Connivance of Bank Employees with Outsiders** | **Preventive / Curative Measures Already Existing/Suggested** | **Action-point assigned to** |
|---|---|---|
| i) Bank employees and unscrupulous persons join hands to open fictitious accounts by impersonation and without proper establishment of identity. Thereafter, such accounts are utilized for giving false credit and withdrawing money there from. | a) Accounts should be opened invariably after establishing the identity of the prospective account-holder. KYC has to be complied without fail.<br>b) High value transactions in such accounts soon after opening are to be scrutinized properly by authorized officer of the branch.<br>c) Collection of instruments in such accounts are to be carefully monitored, particularly when dividend warrants/ interest warrants of substantial amount are deposited for collection. | Hall-incharge/ Manager Accounts with concerned staff. |
| ii) Employees often arrange for outside persons to withdraw money from accounts of different persons, where the arranged person impersonates the actual accountholder | ii) While making payment in such cases, it has to be ensured that the money is received by the actual account holder or by a person authorized by the account holder to receive such money. | Hall-incharge/ Manager Accounts with concerned staff. |
| iii)a) Employees often collude with outsiders in issuing Demand Drafts without obtaining consideration | iii)a) This method is often resorted to by debit of "Suspense / Collection Account" and hence this account has to be carefully scrutinized regularly by senior officers of the branch to prevent the fraud. | Hall-incharge/ Manager Accounts with concerned staff. |
| iii)b) Blank Drafts are handed over to outsiders to note the details thereon and with the help of this spurious Draft leaves are printed outside to be used for siphoning off Bank's money | iii)b) The best method of preventing this type of fraud is to keep the blank draft leaves as well as paid drafts under proper custody so that the same do not | Hall-incharge/ Manager Accounts with concerned staff. |

| | | |
|---|---|---|
| | fall in the hands of unauthorized persons. | |
| iv) Officers often knowingly discount forged/ accommodation bills without underlying trade transactions. | iv) Bills offered for obtaining credit facilities must be scrutinized carefully and possibility of accommodation has to be obviated. | Manager Advances with Branch Head |
| v) Multiple financing to the same party against same security | v) The controlling office/inspectors *of* branches must carefully scrutinize such financing and report when such incidents come to their notice. | S&C Corporate Headquarters through Concurrent & RBIA auditors. |
| vi) Sometimes fake Title Deeds are taken from prospective borrowers as securities. | vii)(a) Title Deeds must be verified and certified by Bank's empanelled lawyers.<br>b) Collect certified true copy of the Title deed from the Registrar and compare it with the original to ascertain its genuineness.<br>c) Branch officials should visit and verify the collaterals and enquire from the persons residing in that locality/neighborhood and record it in the pre/post sanction visit report. | Manager Advances with Branch Head |
| vii) NRI Accounts<br>a) Not obtaining prescribed documents.<br>b) Opening account in fictitious names by depositing foreign | viii) Reserve Bank guidelines regarding opening and handling of NRI accounts have been circulated and all concerned are to scrupulously follow the same guidelines. | Forex-incharge / Hallincharge/ Manager Accounts with concerned staff. |
| currency notes/traveler's cheques.<br>c) Allowing credit of resident funds to non-resident accounts | | |

6.2. **Fraud Risk Measures: As Early Warning Insights**. It is hoped that the above Fraud Risk Measures would help in improvement of deficiencies in the existing processes/ systems besides in fraud risk mitigation. These would also help in early warning insights for strategic and operational decision and management of enterprise-wide fraud risks.

6.3. **Compliance to Extant Regulatory Requirements**. In prevention of frauds, the bank is committed to conduct its banking operations in a fraud-free environment by ensuring strict compliance to the highest possible ethical and professional standards and strive to prevent the bank being used , intentionally or unintentionally , for committing of frauds. The bank shall adhere by all extant rules including those of the RBI, Government of India and other local regulations applicable to various business units as per the local regulations / jurisdiction in which these operate.

6.4. **Implementing & Monitoring Fraud Risk Controls : Functional Responsibility**.

For effective implementation and monitoring of above fraud-risk controls, the three S&C Divisional Heads would be responsible for their respective operational areas / business units and they will be required to submit quarterly

certificates that all the measures on fraud prevention/ control and detection circulated and issued by Vigilance Department/ S&C Corporate Headquarters are strictly complied with.

### 7. Developing a Sound Ethical Culture : An Inseparable Pillar of Fraud Risk Managment .

The bank has always strived to conduct its business on a sound ethical edifice. To further improve ethical values , ―Ethical Code of Conduct /Behavior of J&K Bank Employees‖[12] was for the first time introduced in the ―Policy Framework on Fraud Risk Management & Vigilance (2017-18 version), which imbibes broad universal codes of conduct of business like integrity, inclusive working environment, impartiality, transparency and accountability, feeling empowered during the course of interaction with the cross-section of stakeholders etc. To take forward these principles, the bank with its top management and staff at operational/ other levels would continue to :

a) Adhere to the mission statement of its core/ other business;

b) Adhere to the development of an anti-fraud/ anti-corruption culture so that the bank is externally viewed as a responsible corporate entity;

c) Adhere to the covenants of anti-fraud regulatory directions and will have zero tolerance for fraud incidents . All staff will proactively strive-&-stand for fraud-free business environment & culture by strict compliance to extant systems & procedures and report any suspected incident of fraud or events having fraud-like elements in a responsible way through whistle-blower mechanism and they will be jointly and severally responsible for non-escalating of such incidents;

d) Be seen committed to anti-fraud / anti-corruption goals in both words and actions.

e) Will remain updated about fraud risk/ fraud-prone areas of banking business and would share their knowledge, skill levels, and conduct awareness for all employees and key business partners; and

f) Use bank‘s internal and external inspectors/ auditors for an aggressive-&-comprehensive audit of fraud vulnerable areas / fraud risk areas.

### 8. Strengthening of Sound Internal Control Systems & Compliance Culture.

Internal control systems, comprising of all those policies-&-procedures, processes, access restrictions, transaction controls, physical security etc., which include the division of responsibilities, and checks-&- balances, need strict adherence to reduce fraud risks. Although fraud incidents occur across organizations of all sizes, sectors and locations, yet it is seen that the careful and vigilant staff at grass-root/ other levels act as effective deterrent in prevention and detection of frauds. With increase in business volume and exponential growth of branch network of the bank, the fraud control environment needs to be re-visited so that there is complete fraud-free environment and judicious efforts with visible results are taken to upgrade overall compliance culture to higher level / degree for addressing fraud-vulnerabilities and risks. Wherever possible, the staff at various operational levels must report all fraud-warning signals and alerts as responsible stakeholder for arresting/ minimizing fraud incidents in the bank. ***They will be required to act as main stakeholders against suspected/ actual/ potential frauds.*** Fraud alerts, described as specific events, or red flags, which may indicate ensuing fraud incidents/ events Some examples of fraud red flags are tabulated at Para 6 (A to E) above.

### 9. Some of the Fraud Detection Tools and Techniques: Working Tips for Divisional S&C Heads/ S&C Corporate Headquarters.

The general tools and techniques for identifying possible fraudulent activity include:

[12] Reproduced for ready reference as **annexure "B"** in this framework document.

- Ongoing risk Assessment. Continuous monitoring of operations of business unit with an understanding and educating attitude would not only willingly rope in all staff as active stakeholders in prevention and detection of frauds but also make this exercise as business-supportive and pro-staff.

- Trend Analysis. Data on fraud trends is periodically disseminated through different advisories including sharing of modus-operandi of latest fraud incidents in the banking industry. This needs to be studies in detail for meaningful insights for sharing with staff periodically so that they remain updated about latest trends in the banking / financial sector.

- Data Matching. Both on-line and off-line data matching with or without use of requisite software would enable our S&C Divisional Heads to pick up threads / clues of fraud-like incidents from the system / using MIS as a key resource. With the use of Enterprise-wise Fraud Risk Management software in near-future data matching and data-mining for picking up fraud-like incident-threads would become a reality for all three Divisional S&C Heads for real time monitoring.

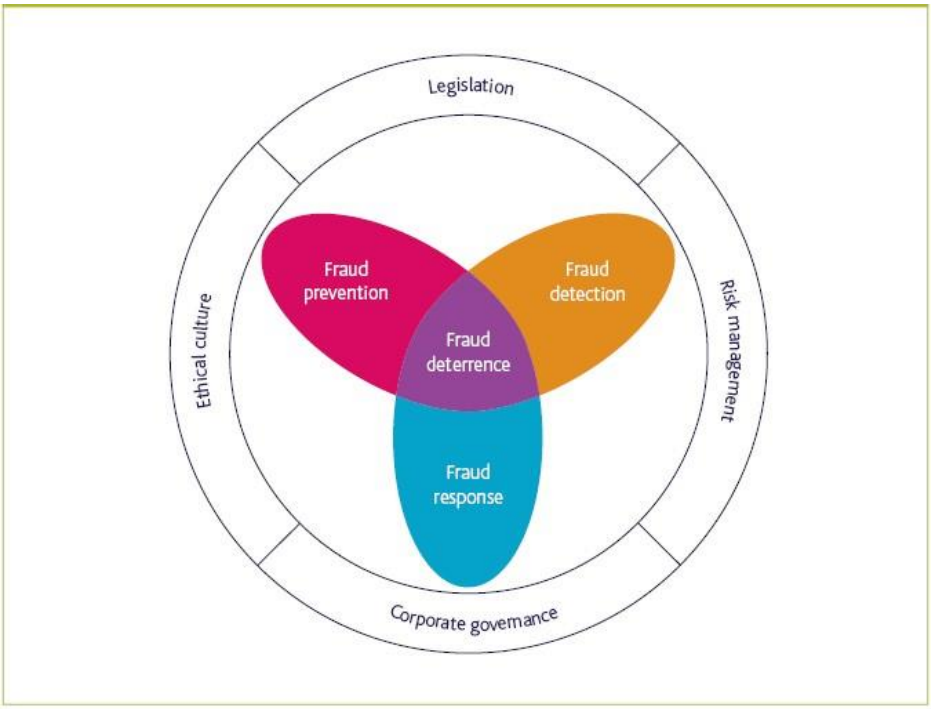
- Exception Reporting. The S&C, Corporate Headquarters will be advising the Information System Auditors to check and analyze Exception Reports on continuous basis as a fraud-deterrence measure.

- Internal (RBIA) / Concurrent Audit. Both these audits have a central role in detection of fraud incidents so that the time-lag in occurrence and detection of a fraud incident are substantially curtailed and all fraud incidents are detected without any delay.

- Reporting Mechanisms. The extant reporting system under different systems including whistle-blower mechanism besides Internal (RBIA) / Concurrent Audit as given above will continue to be the main internal modes of reporting fraud incidents.

## 10. **Fraud Deterrence: Overall Framework**

Different anti-fraud aspects of a fraud strategy, as shown in the diagram below, are closely interlinked. Each plays a significant role in combating fraud, with fraud deterrence at the centre. Fraud detection acts as a deterrent by sending a message to likely fraudsters that the organization is actively fighting fraud and that procedures are in place to identify any illegal activity. The possibility of being caught will often persuade a potential perpetrator not to commit a fraud. The other complementary detection methods given above will go a long way in countering / minimizing the impact of fraud incidents on the bank. Added to it, the consistent and comprehensive use of the fraud risk response (FRR) measures enumerated above to suspected and detected fraud incidents, would send a clear message that occurrence of any fraud incident is taken very seriously by the bank & its staff and that action will certainly follow against the perpetrators. Each case that is detected and investigated would reinforce this deterrent posture and act as a form of fraud prevention.




11. **Fraud Risk Deterrence : Staff Training and Awareness Aspects.**

Almost every time a fraud occurs, many people who were unwittingly close to it, are shocked that they had no idea it was going on. It is therefore important to raise awareness through education and training. Particular attention needs to be paid to employees working in high risk areas (advances/ clearing and transaction processing) and operations who have a central role in the prevention and detection of fraud. The bank would be conducting training / fraud awareness programs on continuous basis which will highlight the key & critical aspects in different functional areas of the staff for preventive vigilance. As generally, fraud is often discovered through a tip-off, it is therefore essential that all employees understand what constitutes fraud, how to identify it and how they should respond. Appropriate training/ awareness is more likely to reduce the risk of fraud. The training methods may include:

- formal training sessions;
- group meetings;
- posters, employee newsletters and Intranet content.

Communication from Vigilance Department, Corporate Headquarters has to be clear and ongoing to keep pace with the changing fraud trends in the banking industry. However, the training & awareness has to be not only well-focused but also balanced positively with achievement of business targets / goals so that the staff do not get de-motivated in taking normal business risks.

12. **Fraud Risk Deterrence : Role of Whistle-blowing as an Effective Mode of Reporting Suspected/ Actual/ Potential Fraud Incidents.**

The bank has already set-up whistle –blowing (copy of the document given as annexure ―C‖) which the staff would be advised to use mandatorily in escalating any suspected/ actual/ potential fraud incident in the areas of the workings so that the top management gets timely inputs.

13. **Preventive Vigilance Framework : Pyramidal Roles & Responsibilities from Top to Bottom .**

| Name of the Functionary of the Bank | Role in Preventive Vigilance Framework |
|---|---|

| | |
|---|---|
| **Audit Committee of the Boardand Special Committee of Board on Frauds.** | To monitor on a regular basis the Bank‘s approach to tackling fraud and corruption and promote an anti-fraud Strategies and Culture. |
| | |
| **Chief Executive** | Ultimately accountable for the effectiveness of the Bank‘s arrangements for countering fraud and corruption. |
| **CVO** | To ensure the Bank has adopted an appropriate antifraud strategy, there is an effective internal control environment in place and there is an adequately resourced and effective Internal Audit and Corporate Anti Fraud Set-up for _counter-fraud‘ measures. |
| **3 Divisions of the S&C (Kashmir, Jammu & Delhi) together with Vigilance Department, Corporate Headquarters & Zonal Law Departments / Law Department, CHQ.** | To advise and guide the Bank and its staff on anti-fraud strategies as per the best-industrial practices in vogue and extant Regulatory guidelines to ensure that the Bank operates within the legal and statutory Codes of Practice. |
| **External Audit** | Statutory duty to ensure that the Bank has adequate arrangements in place for the prevention and detection of fraud, corruption and theft. |
| **Internal Audit** | Internal audit is responsible for evaluating the potential for the occurrence of fraud and how the organization manages fraud risks. |
| **Fraud Risk Management Group (FRMG)** | Manage the risk of fraud and corruption. To promote staff awareness and ensure that all suspected or reported irregularities are immediately referred to related department (S&C, CHQ/Vigilance/Information Audit/Legal Audit/ Forensic Audit and to ensure that there are mechanisms in place within their service areas to assess/ detect/ mitigate the risk of fraud, corruption and theft and to reduce these risks by implementing strong internal controls. |
| **Employees / Bank Staff** | Bank‘s employees are the first line of defence against fraud and corruption. They are expected to conduct themselves in ways which are beyond reproach, above suspicion and fully accountable. Also responsible for reporting malpractice through well established _whistleblowing‘ procedures. Employees are expected to adhere to the Employee Code of Conduct, Financial Regulations and extant procedure/rules as per the RBI/ SEBI/ Prevention of Corruption Act 1988 (PCA)/ Prevention of Money Laundering Act, 2002 / BR Act etc. Besides, they must comply with the Code of Conduct and related Bank‘s policies and procedures, to be aware of the possibility of fraud, corruption and theft, and to report any genuine concerns accordingly. |

**14. Periodic Review Preventive Vigilance Framework.**

A review of the ―Preventive Vigilance Framework with Special emphasis on Activation and Promotion of Whistleblower Policy[13]‖ and ―Policy Framework on Fraud Risk Management & Vigilance‖ would be made from time to time as per the business needs of the bank.

**15. Concluding Remarks on Preventive Vigilance Framework.**

An effective anti-fraud strategy has four main components, namely, (a) prevention ; (b) detection ; ( c) deterrence, and (d) response with operates within the overall framework of risk management, responsible corporate governance, sound ethical culture and healthy legislative set-up with all pervasive commitment-&-efforts to root-out fraud incidents. In case any fraud incident with suspected or real takes place, there is need to examine its causative factors in a comprehensive manner so that the weak-vulnerable areas are fixed once for all and recurrence of similar incidents is ruled out forthwith.

[13] Given as annexure ―F‖.

# Annexure "A" : Comparative Data on Fraud Incidents upto 30.09.2018

| Year | Upto Rs1.00 lakh | | | | | | Above Rs1.00 lakh | | | | | | Total | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total Frauds | | Credit Related Frauds | | Percentage | | Total Frauds | | Credit Related Frauds | | Percentage | | Total Frauds | | Credit Related Frauds | | Percentage | |
| | No. | Amount Involved in Lakhs of Rs. | No. | Amount Involved in Lakhs of Rs. | No. | Amount | No. | Amount Involved in Lakhs of Rs. | No. | Amount Involved in Lakhs of Rs. | No. | Amount | No. | Amount Involved in Lakhs of Rs. | No. | Amount Involved in Lakhs of Rs. | No. | Amount |
| 2014-15 | 5 | 2.86 | 2 | 0.75 | 40 | 26.22 | 7 | 90286.68 | 6 | 90186.68 | 86 | 99.89 | 12 | 90289.54 | 8 | 90187.43 | 67 | 99.89 |
| 2015-16 | 3 | 1.25 | 0 | 0 | 0 | 0 | 16 | 1238.47 | 8 | 1089.29 | 50 | 87.95 | 19 | 1239.72 | 8 | 1089.29 | 42 | 87.87 |
| 2016-17 | 2 | 1.62 | 0 | 0 | 0 | 0 | 23 | 31165.02 | 16 | 30981.28 | 70 | 99.41 | 25 | 31166.64 | 16 | 30981.28 | 64 | 99.41 |
| 2017-18 | 4 | 1.59 | 0 | 0 | 0 | 0 | 14 | 21510.46 | 12 | 21505.38 | 86 | 99.98 | 18 | 21512.05 | 12 | 21505.38 | 67 | 99.97 |
| 2018-19 | 1 | 0.35 | 0 | 0 | 0 | 0 | 3 | 12097.64 | 2 | 12068.2 | 67 | 99.76 | 4 | 12097.99 | 2 | 12068.2 | 50 | 99.75 |

## Annexure "B": Ethical Code of Conduct/ Behavior of J&K Bank Employees

i) **Codes of Conduct: Introduction**. Codes of Conduct or Codes of Behavior are designed to anticipate and prevent certain specific types of behavior; e.g. conflict of interest, self-dealing, bribery, and inappropriate actions. The rational for a written code is that it is necessary to both protect the employee while at the same time protecting the reputation of the bank and its various stakeholders. Standards of Conduct do change over time but it is sometimes useful to look at historical standards in order to recognize that the behavioral problems are often similar over time but technology or social circumstances can have a profound impact on actions that are prohibited. **ii) Main Parameters of Our Ethical Code of Conduct / Behavior .**

1) **Integrity** underpins everything that we do at the Bank. We want to ensure that the Bank is a place where people always do the right thing for the institution and our mission. It is a place where we all collaborate and support each other in working for the public good.–
2) The Bank has an **inclusive working environment** where difference is celebrated and discrimination or harassment is not tolerated.
3) We **act with impartiality**. We want to be objective in our decision-making and decisive in our actions.
4) Our nature of services necessitate us **to be open and accountable** for our actions and for the resources we use.
5) Finally, we should **feel empowered** to hold each other to account. We believe that, in all of our interactions with each other, with external stakeholders and with Union Territory of J&K / Central Government/ RBI/ other regulators , we have an opportunity to enhance public trust in what we do and set the best ethical and professional tone for the financial services industry we operate into.
6) We should all feel encouraged and empowered to make positive suggestions, and our expectation is that each of us would do so when necessary, including challenging what we do or how we do it if we see a conflict with our values and our Code. We would encourage our colleagues to _Speak up' if they believe that our Code is being breached.
7) Our Code applies to all of us (all stakeholders of the bank) including all bank colleagues from across the full range of the business.
8) The values and the expectations embodied in our Code are not new. Our Code encompasses our core ethics policies; seeks to highlight, bring together, and update certain other key existing policies we all are already familiar with and provide context for them.
9) Living within our Code is not simply about observing the letter of the policies referred to in it; they cannot provide for every contingency. We aspire to set an example of the best in banking service: complying with our Code is about understanding and embracing the principles and spirit behind it. In doing so, each of us will make our individual contribution to the Bank's business objective and strategic policies and decision to achieve all business targets in sync with the corporate responsibility that we owe to the individuals and entities outside the bank.
10) Our Code represents our commitment to how we work at the Bank and how we should conduct ourselves (both within and outside the Bank). It applies to all of us i.e. to all employees at operational and administrative/ management level.
11) Our Code will be publicly available on bank's intranet and provides a statement about the behavior our colleagues, counterparties, stakeholders and the public should expect from us.
12) Our Code is based on ***five principles***. These represent the spirit of our Code. These are briefly listed below:

- **Acting with integrity**

Integrity is one of the principles of public life, closely related to the principles of selflessness and objectivity. Our personal interests should never influence our decisions at work, and we must be free of any suggestion of inappropriate influence**.**

- **Creating an inclusive Working Environment.**

We stand for an inclusive environment, and we welcome the benefits that diversity brings. We want an environment where all colleagues feel comfortable being themselves. We support diversity as part of what we do every day. We established our Bank wide values in the Strategic Plan: collaborative, inclusive, decisive, open and empowering. These are embedded in our performance management and development approaches. Both what we do and how we do it, contribute to our performance as individuals and as an institution. We believe in inclusive and collaborative behaviors. We believe in a meritocracy where all get developed, promoted and rewarded fairly. We have a well-established grievance procedure as well as the option for colleagues under whistle-blower framework. Any of us who believe that we have been discriminated against, harassed or bullied or have seen anyone else be the victim of discrimination, harassment or bullying, should feel empowered to raise the matter through appropriate forums/ means provided by the bank.

- **Demonstrating Impartiality.**

We take pride in the quality and impartiality in our dealings and functioning . We engage with others professionally and make decisions fairly and on merit, using the best evidence available and without bias. We recognize that impartiality and objectivity are crucial to the decisive behaviors that form a core part of our Bank values. We know that our reputation for impartiality and independence is vital to our effectiveness, and, if lost, would be hard to recover. Like other colleagues in the banking industry, we know we must be seen to be apolitical and must never allow ourselves to become open to the perception that our decisions have been inappropriately influenced.

- **Being open and Accountable.**

We want to be open and accountable to each other and in our dealings with all our stakeholders including our valued customers .We know our decisions and actions both as individuals and a corporate entity are subject to public scrutiny and we must welcome and facilitate that scrutiny. Open behaviors, practiced every day by all of us, are a core Bank value and are integral to the success of the Bank and its business objectives. We are responsible for the resources and information entrusted to us in the work we do and we have to be accountable for managing those with due care, skill and diligence. We are accountable for engaging with our colleagues constructively and recognize when we should reach out to them. Good record keeping is vital; records represent our institutional memory and allow for proper questioning. In the course of our work at the Bank we make critical policy, supervisory and operational decisions that have a broad impact. We are ultimately accountable to the various stakeholders of the bank for those decisions and we owe it to them as well as to ourselves and each other to properly and securely maintain our records. We all have a responsibility to ensure our records are authentic, accurate, timely, complete, appropriately classified, and retained in line with our records management policies. At the Bank we have access to a wide variety of information which exists in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation, including information regarding access to systems and software versions, processes and passwords. In the wrong hands that information could be used to disrupt or damage our ability to pursue our business objectives. We all have a responsibility to protect that information. When accessing Bank information electronically, we should only use the Bank‘s devices and systems and Bank-approved software. We must use these safely and securely.

- **Feeling Empowered.**

One of the five values in our Strategic Plan is empowerment and one key aspect of that, the ability to speak up through Whistle-blower mechanism about something that is causing us serious concern, is embedded in our Code. Each of us should feel encouraged to raise serious issues or concerns, whether they relate to the behavior or practice of a colleague which we believe might be in breach of our Code, or to information that could suggest misconduct by external market participants. Our values explicitly seek to encourage an environment where a diversity of opinions and views are brought to bear on all the decisions we need to make. Our approach to performance management recognizes that how we do our work is as important as what we do, and we should all feel encouraged to raise concerns if we feel our values are not being adhered to.

We want to make sure that everyone fully understands what is expected of them and what they need to do to adhere to our Code.

***<u>Failure to comply with our Code and its associated  principles / policies could lead to disciplinary action.</u>***

## Annexure "C": Whistle Blower Policy.

### 1. Introduction& Objective of

1.1. Consistent with its long term business strategy, the Jammu & Kashmir Bank Limited, a regulated entity, is committed to adopting of the highest possible standards of business governance, ethics, regulatory-compliance and related codes of conduct (including Code of Conduct for the Board Members and Senior Management Personnel, the Insider Trading Code, the Ethical Corporate Policy for Acceptance of Gifts, Fair Practice Code etc.) for carrying on its business in a transparent manner with the utmost integrity and accountability at all levels. The bank is also committed in its dealings with its all stake holders/general public to a transparent business ethos & culture wherein it is safe & acceptable for all employees, directors and other specified stakeholders to voice / raise their genuine concerns in good faith and in a responsible & effective manner, by providing a framework to promote responsible vigilance mechanism **through a whistle blowing mechanism** to safeguard the bank against internal/ external threats like frauds, bribery, corruption, abuse of authority, noncompliance to regulatory guidelines, non-adherence to extant systems & procedures involving financial and/ or reputational loss through the process of ―participative vigilance‖.

1.2. To further enhance the transparency in the organization by encouraging the employees/directors/other specified stakeholders to report any wrongdoing, which comes to their knowledge in the day-to-day performance of their duties or interaction with other fellow-colleagues/ bank staff without fear of retaliation, victimization and unfair-treatment, the Bank has formulated the **„Whistleblower Policy"** to guarantee them protection from any adverse departmental proceedings. The Policy is compliant to regulatory requirements under Section 177 (9) of the Companies Act 2013, and Clause 49 of Equity Listing Agreement as amended by the Securities and Exchange Board of India vide its circular No. CIR/CFD/Policy Cell/2/2014 dated April 17, 2014.

1.3. It is also expected that this Policy will encourage Bank's employees, directors and other specified stakeholders, to bring to the notice of the management any issue involving compromise/ violation of ethical norms, legal or regulatory provisions, etc. which is in their knowledge, without any fear of retaliation against them. The policy neither releases directors and employees from their duty of confidentiality in the course of their work, nor is it a route for taking up a grievance about a personal situation.The main intent of the policy is to ensure that Bank continues to strive to the highest possible standards of ethical, moral and legal Business Conduct and its commitment to open communications. However, a disciplinary action if any, taken against the Whistle Blower which has occurred on account of poor job performance or misconduct by the Whistle Blower, shall not be protected under this policy. For the sake of absolute clarity, it is specified that the Whistle Blower Policy does not tantamount, in any manner, to dilution of the vigilance mechanism in Bank. Any Protected Disclosure made by a whistleblower under this policy, if perceived to have a vigilance angle, shall be referred to Chief Internal Vigilance Officer (CIVO) of the Bank.

### 2. Applicability of Policy & Its Effective Date.

This policy which has been in existence, as amended from time to time, applies to all directors, employees including those who are on probation/contract or any other person that the Bank through its Audit Committee of Board may wish to extend this policy to including a supplier, vendor, service provider who in good faith raises a genuine concern or report incidence of any activity by the bank or its employee or director that may constitute an event of concern. The effective date of the policy will be the date it is approved by the Board of Directors and/or put in public domain.

### 3. Definitions of Key Terms.

The definitions of some of the key terms used in this Policy are given hereunder. However, terms not defined herein shall have the meaning assigned to them under the relevant Code/service Rules.

a. **"Audit Committee"** means the Audit Committee of Directors constituted by the Board of Directors of the Bank, in accordance with Section 177 (9) of the Companies Act 2013, and Clause 49 of Equity Listing Agreement as amended by the Securities and Exchange Board of India vide its circular No. CIR/CFD/Policy Cell/2/2014 dated April 17, 2014.

b. **"Bank"** means The Jammu & Kashmir Bank Limited.

c. **"Employee"** means every person in the employment of the Bank and the directors.

d. **"Code"** means the Code of Conduct for the Board Members and Senior Management Personnel, The Insider Trading Code, The Ethical Corporate Policy for Acceptance of Gifts, The Fair Practice Code and The Ethical Standards Employed by the Bank.

e. ―Chief Internal Vigilance Officer (CIVO)‖ means the executive heading the Vigilance Department of the Bank at Corporate Head Quarters, Srinagar, J&K (either Vice-President or President or Senior-President or Executive President, whosoever is functional on the senior-most position in the Vigilance Department at any point of time).

f. **"Director"** means every Director for the time being on the Board of Directors of the Bank.

g. **"Investigator"** means any person/agency authorized, appointed, consulted or approached by the CIVO/Chairman of the Audit Committee of Board of Directors (also referred to as Chairman AC BoD hereinafter) and also includes police and other government investigating agencies.

h. **"Protected Disclosure"** means any communication made in good faith or in overall interests of the Bank that discloses or demonstrates information that may evidence unethical or improper activity including issues/concerns as given under (k) below.

i. **"Subject"** means a person against or in relation to whom a Protected Disclosure has been made or evidence gathered during the course of an investigation.

j. **"Whistleblower"** as given above includesany person in employment of the Bank or director or any other person/entity that the Bank through its Audit Committee of Board may wish to extend this definition to; reporting a ‗protected disclosure' under this Policy. It will also include a supplier, vendor, service provider who in good faith raises a genuine concern or report incidence of any activity by the bank or its employee or director that may constitute an event of concern as given under (k) below.

k**) "Issues and/ or Concerns"** will include events/ instances/ incidence of any one or more of the following/ other similar cases:-

i. instances of corporate fraud; ii. unethical business conduct; iii. a violation of Central or State laws , rules, regulations and/ or any other regulatory or judicial directives; iv. any unlawful act: whether criminal or civil; v. malpractices; vi. serious irregularities; vii. impropriety, abuse or wrong doing; viii. deliberate breach and non-compliance with bank's policies; ix. suspected/committed criminal offence; x. non adherence of KYC/ AML guidelines &related issues; xi. bank funds used in an unauthorized manner; xii. sexual or physical abuse of a service recipient, service provider, etc.

xiii. discrimination against a service recipient, service provider, etc. on grounds of sex, caste, religion or disability;

xiv. any action/s which endanger the health or safety of employees, customer, general public etc. xv. concealment of any information which is detrimental to the interests of the Bank.

xvi. actions which may endanger financial position and/or reputation of the Bank and any of its stakeholders;

xvii. questionable accounting/ audit matters, financial malpractices; and xviii. any other form of improper action or conduct.

**4. False or Bogus Allegations / Disclosures with malafide.**

It shall be ensured that genuine whistleblowers are accorded complete protection from any kind of unfair treatment or adverse departmental proceedings. However, any abuse of this protection will warrant suitable action including reprimand. The protection under this policy would not mean protection from disciplinary action arising out of false or bogus allegations made by a Whistleblower knowing it to be false or bogus or with a *mala fide* intention.

**5. Scope**

5.1. The policy is intended to help the Bank to fulfill its commitment with all stakeholders so that its dealings with them will stand for strong ethical principles of integrity and transparency. This objective can be obtained when all the stakeholders including employees contribute towards this policy by reporting the wrongdoings including issues/concerns as given under 3(k) above which they may notice within the organization, without any fear/reprisal/retribution.

5.2. The policy is primarily for preventing financial & reputational losses to Bank and all its stakeholders. No employee should report his/her personal grievance/s under the policy, as proper grievance redressal mechanisms for employees are already in place in the Bank.

5.3. The disclosures made under this policy will be appropriately dealt with by the Bank, and shall be reported to the **Audit Committee of the Board which will be the monitoring authority for the purpose of this policy**.

5.4. If any of the members of the Audit Committee of the Board shall have a conflict of interest in a given case, he/she should rescue himself/herself and other members of the Committee would deal with the said matter.

**6. Whistle Blower"s Role**

6.1. The whistleblowers' role is that of a reliable information reporter. He/she is not required or expected to act as investigator or fact finder, nor would he/she determine the appropriate corrective or remedial action that may be warranted in a given case.

6.2. The whistleblower should not act on his/her/its own, in conducting any investigative activities, nor does he/she/it have a right to participate in any investigation other than as may be required by the Investigator/Designated Authority or the Audit Committee of the Board.

**7. Procedure for Reporting**

7.1. The detailed procedure for lodging of complaint under ―Whistle Blower Policy‖ is given under:-

7. **a) For lodging the complaint off-line (i.e. in physical format).**

i. The complaint must be in a closed / sealed envelope. ii. The envelop should be addressed to the ―Chief InternalVigilance Officer/ Chairman Audit Committee of Board‖, as the case may be,with superscripted words**"Complaint under Whistle Blower Policy."**If the envelop is not super scribed-&-closed/sealed as above, it will not be possible for the Chief Internal Vigilance Officer/ Chairman of Audit Committee of the Board to protect the identity of the complainant and the complaint will be dealt with as per the normal complaint handling policy of the bank. iii. The complainant should give his / her name & address in the beginning or at the end of the complaint or in separately attached letter.

iv. The Chief Internal Vigilance Officer/ Chairman of the Audit Committee of the Board will not normally entertain any anonymous / pseudonymous complaint under this Policy. Any anonymous / pseudonymous complaints will be routed through the Customer Care/ S&C/ Vigilance Departments of Corporate Headquarters, as the case may be as a normal complaint & will be dealt with by those departments as per their extant/ applicable guidelines.

v. The text of the complaint should be carefully drafted, specific and verifiable. vi. To protect the identity of the complainant, the Chief Internal Vigilance Officer/ Chairman of the Audit Committee of the Board will not issue any acknowledgement and the whistle blowers advisably shall not enter into any further correspondence with the Chief Internal Vigilance Officer/ Chairman of the Audit Committee of the Board in this respect or in their own interest. The Chief Internal Vigilance Officer/ Chairman of the Audit Committee of the Board shall ensure that subject to the facts of the case being verifiable, necessary action will be taken on the complaint as provided in this policy and/or as per other extant guidelines of the bank. vii. If any further clarification is needed, the Chief Internal Vigilance Officer/ Chairman of the Audit Committee of the Board will get in touch with the complainant.

viii. **All „protected disclosures‟ concerning financial/accounting matters should be addressed to the Chairman of the Audit Committee of the Bank**.

ix. In respect of all other _protected disclosures‘ not relating to financial/accounting matters inculpating Vice Presidents and above should also be addressed to the Chairman of the Audit Committee of the Bank;
and those inculpating other employees should be addressed to the Chief Internal Vigilance Officer of the Bank who will be reporting to the Audit Committee.

x. The contact details of the Chairman of the Audit Committee and the Chief Vigilance Internal Officer of the Bank are, as under:

| | |
|---|---|
| **The Chairman Audit Committee of Board Board Secretariat, CHQs M. A. Road Srinagar** | **Chief Internal Vigilance Officer, Vigilance Department, CHQs M. A. Road Srinagar.** |

The _protected disclosures‘ should be factual and not speculative or in the nature of a conclusion, and should contain as much specific information as possible to facilitate proper assessment of the matter and the urgency for investigation.

xi. The whistleblower should furnish a brief _note‘ covering the pertinent details about the matter that he/she wishes to report. This _note‘ may, inter_alia, cover the following aspects to the extent possible:-

- Wrongdoing to be reported.
- Name/s with particulars of wrongdoer/s.
- When it occurred?
- Specific location where the wrongdoing occurred.
- How the alleged wrong doer committed the alleged wrongdoing (if conversant with the modus operandi)?
- Why the whistleblower believes the activity to be improper?
- Names of the witnesses (if any) to the alleged wrongdoing. ➢ Documentary evidence, if any, to be attached.

However, the whistleblower should not here mention his name or any other particulars that may disclose his/her identity from the contents of the complaint.

**7. b)<u>For Lodging the Complainant on-line on J&K Bank Intranet/Internet Portals (already available).</u>**

The bank will set-up **<u>"Whistle Blower" module</u>** on J&K Bankinternet/intranet portals to facilitate lodging of on-line complaints under ―Whistle Blower‖ category to Chairman AC BoD/CIVO, as the case may be. The access rights to view the on-line complaints under ―Whistle Blower‖ category willbe restricted to the designated authorities' i.e. Chief InternalVigilance Officer/ Chairman of the Audit Committee of the Board / the authorized official expressly authorized in this regard by Chairman AC BoD/CIVO to be called the ―Authorised Person‖. The Authorised Person in this regard shall not be below the rank of Vice-President in the Vigilance Department. This will ensure protecting the identity of the complainant as also confidentiality of the contents since there will not be any intervention/ handling by a third person during the transit-phase.

**8. <u>Role of the Chief Internal Vigilance Officer / Chairman of the Audit Committee of the Board</u>.**

a. The Chief Internal Vigilance Officer/ Chairman of the Audit Committee of the Board will be designated authorities to receive complaints made by any officials/ employees / directors / specified third parties of the bank including the subsidiaries / affiliates/ sponsored bank.

b. The Chief Internal Vigilance Officer/ Chairman of the Audit Committee of the Board, as the designated authorities, will ascertain from the Whistleblower whether he/she/it has made the disclosure/complaint. If the complaint is anonymous / pseudonymous, the authority shall not take any action in the matter under ―Whistle Blower Policy‖ but may, if deemed fit, refer the complaint to the concerned department (Custome Care Division, S&C or Vigilance Departments of Corporate Headquarters) as per apparent contents / escalated-issues of the complaint.

c. The identity of the complaint will not be revealed unless the complainant himself has made either the details of the complaint public or disclosed his identity to any other officer or authority.

d. If the allegations made in the complaint referred to theChairman of Audit Committee of Board are specific and verifiable then he/she(Chairman of Audit Committee of Board) may refer the same to the CIVOfor further action. As regards the complaint made to the Chief Internal Vigilance Officer where the allegations are specific and verifiable, he/she will take further action in the matter.Further action in this context would include ordering an investigation/inquiry into the complaint and obtaining all the relevant papers / documents in respect of the matter raised in the complaint. While calling for preliminary inquiry/ investigation report, the CIVO/Chairman AC BoD will not disclose the identity of the complainant. The CIVO/Chairman AC BoD will also advise the authority/ies from whom the report is sought to keep the identity of the complainant secret/ confidential, if for any reason, the said authority comes to know about the identity of the complainant. In case the identity of the complainant gets disclosed despite directions of the CIVO/Chairman AC BoD, such appropriate action as deemed fit by the CIVO/Chairman AC BoD will be taken against the person responsible for that disclosure.

e. If any whistleblower is aggrieved of any action on the ground that he/she/it is being victimized due to the fact that he/she/it had filed the complaint, he/she/it may file an application before the Chief Internal Vigilance Officer/ Chairman of Audit Committee of the Board seeking redressal in the matter. Chief Internal Vigilance Officer / Chairman of Audit Committee of the Board will ensure that no punitive action is taken by any concerned authority against that person <u>on perceived reasons of being a ―whistle blower.‖</u>

f. In case the CIVO/Chairman AC BoD finds the complaint to be motivated or vexatious, he/shemay recommend initiation of action against such complainant as per extant rules.

g. After conducting investigation, if it is revealed that there was misuse of office and/or contents &substance in the allegation/s, the CIVO/Chairman AC BoD shall recommend appropriate action which shall inter-alia include:

i. *Appropriate proceedings against the concerned staff member/director;*
ii. *Recommending to appropriate authority for initiation of criminal proceedings in suitable cases, if warranted , by facts & circumstances of the case; and*
iii. *Recommend corrective measures to prevent recurrence of such events in future.*

h. In case a complaint results in detection of unethical practices/ abuse of authority / official position, fraud and other wrong actions and thereby averts or minimizes the financial and/or reputational loss to the bank, the moral courage shown by the ―Whistle Blower‖ in staff will be recognized by the bank by way of appropriate incentive/ benefit . For this purpose, the CIVO/Chairman AC BoDmay recommend that such genuine informants are given due weightage in career growth and placements as may be considered fit by the Human Resource Development Department (HRDD) of the bank. A confidential dossier will be maintained personally by the CIVO/Chairman AC BoDfor this purpose. The CIVO/Chairman AC BoD will ensure full protection against disclosure of identity of the Whistle Blower.

―To take suitable action and to avoid inordinate delay due to limited meetings of the Audit Committee of the Board, the ACB may appoint an ―Administrator‖ to over-see/monitor whistle blowing mechanism and allow/ authorize him for taking necessary action under the covenants of this policy document. Whether a complaint has been raised through on-line/ off-line mode, the ―Administrator‖ if appointed shall get it probed normally within 15 days and submit a compliance report, only in those cases where some malafide have been established/ proved, to the Committee in the ensuing meeting.‖

**9. Investigation**

9.1. Once a concern has been raised/ reported and ordered to be investigated by the CIVO/Chairman AC BoD, the Authorized Person shall take the following steps:-

i. obtain full details & clarifications about the issue/concern;
ii. recommend investigation of the same by the bank‘s internal auditors or any other investigation agency or person, internal or external including the police;
iii. fully investigate into the allegation with the assistance where appropriate of other individuals/bodies; iv. refer the issue/concern to the Disciplinary Authority for initiation of disciplinary action under rules.

9. 2.All the ‗protected disclosures‘ reported under this policy, if warranted, shall be got thoroughly investigated in a manner deemed appropriate by the Chief Internal Vigilance Officer / Chairman of the Audit Committee of the Board. They shall oversee the investigation under the supervision of Audit Committee of Board. If any member of the Audit Committee has a conflict of interest in any given case, then he/she should recuse himself/herself and the other members of the Audit Committee should deal with the said matter.

9.3. The decision to conduct an investigation taken by the Chief Internal Vigilance Officer / Chairman of the Audit Committee would by itself not constitute culpability or guilt of the subject and is to be treated merely as a neutral fact finding process.

9.4. The investigation will be initiated only if prima-facie it appears that the alleged act reported constitutes an improper or unethical activity or conduct and is supported by required information. However, the investigation itself should not be undertaken with a preoccupied mind that it relates to improper or unethical activity.

9.5. The identity of a _subject' will be kept confidential to the extent possible subject to legal and investigation constraints.

9. 6.The _subject/s' may be informed about the allegations after a formal investigation for his/ their involvement in the fact finding process. If informed, the _subject/s' shall have a duty to co_operate with the CIVO / Chairman of the Audit Committee or any of the Investigator/s during investigation, so long as such co_operation does not compromise the self-incrimination protections available under the applicable laws.

9.7. The _subject' shall have a right to counter the allegations during/ after investigation. If the opportunity is provided by the investigator, he/she should not try to deter or unduly influence the investigation process. He/she should neither destroy, tamper or withhold the evidence nor resort to influence, coercion or intimidation.

9.8. The _subject' will be given the opportunity to respond to material findings of investigation, unless there is no reason therefor. No allegation of wrongdoing against a _subject' shall be maintainable, unless it is substantiated with evidence during investigation.

9.9. The investigation shall be **completed normally within 15 days of the receipt** of the _protected disclosure'.

—i) All Concerns/ Issues investigated under this policy and all information obtained during the course of investigation will remain confidential, except as necessary to conduct the investigation and take any remedial action in accordance with applicable laws/ bank policies.

ii) While investigating the concern raised by the Whistle Blower, the bank may or may not be able to inform such Whistle Blower the precise action/ findings of such investigation. The bank, however, will take all steps to remove the difficulty/ anxiety of the Whistle Blower, which he may experience as a result of raising/ reporting such concern. If the whistle blower is required to give evidence in criminal or disciplinary proceedings, the bank will arrange for the whistle blower appropriate legal advice about the process and procedure to be followed in this regard. Direct access to the Chairperson of the Audit Committee of the Board will be provided to Whistle Blower should the Whistle Blower so require, in appropriate cases.‖

**10Disciplinary Action.**

Audit Committee shall oversee that appropriate disciplinary actions are taken as per the extant guidelines / policies of the bank in an event the complaint is found based on the facts.

**11. Untrue Concerns: Malafide Versus Bonafide Ones .**

If a Whistle Blower reports / raises a concern in good faith, which is not confirmed by subsequent investigation, no action will be taken against him (the Whistle Blower). In making a disclosure, the Whistle Blower shall exercise due care to ensure the accuracy of the information. In case of repeated frivolous complaints being filed by an employee or director (if he/she chooses to disclose his/ her name), the Audit Committee may take suitable action against the employee or director for such malafide intentions/disclosures including reprimand and / or other disciplinary action as deemed fit. However, in case of third party malafide reporting, criminal action may be taken on case-to-case basis and/ or in exceptional cases and at the sole discretion of the Chairman of the Bank in case issues like reputational/ business losses of the Bank or where its staff are involved.

**12. Discrimination.**

The bank strictly prohibits discrimination, retaliation or harassment of any kind against a Whistle Blower who based on his reasonable belief that such conduct or practices have occurred or are occurring , reports that information. If a Whistle Blower believes that he/ she has been subjected to discrimination, retaliation or harassment for having reported Concern under this policy, he/ she must report such fact to any member of the Audit Committee. It is imperative that

the Whistle Blowers bring such matters to the attention promptly so that any Concern of discrimination, retaliation, or harassment can be investigated and addressed promptly & appropriately by Audit Committee of the Board of Directors.

**13. Confidentiality.**

The Whistle Blower, members of Audit Committee or CIVO or the Administrator or investigation person or persons who will be investigating or deciding on the investigation shall not make public the Issue/Concern disclosed. Further, the identity of the whistle blower shall be kept confidential, unless legally required to be disclosed during investigation/s or after investigation/s are carried out.

**14. Protection& Redressal in case of Unfair Treatment of Whistle-blower.**

14.1. There shall be no unfair treatment against the whistleblower for having reported a _protected disclosure‘ in good faith or in overall interests of the Bank under this policy. The Bank, as a policy, condemns any discrimination, harassment, victimization or any other unfair employment practice against whistleblowers. Therefore, complete protection shall be given to whistleblowers against any unfair practice like retaliation, threat or intimidation of termination/suspension of service, disciplinary action, transfer, demotion, refusal of promotion, or any direct or indirect use of authority to obstruct their right to continue, to perform their duties/functions including, making further _protected disclosures‘. If the evidence of whistleblower, in criminal or disciplinary proceedings is mandatory, the Bank will provide the necessary advice to him/her, if any, required. The Bank shall also reimburse the expenses to the whistleblower, if any, incurred by him during this process.

14.2. Any other employee or director assisting in the said investigation shall also be protected to the same extent as the whistleblower.

**15. Investigators to be Impartial.**

The investigators should conduct a thorough and impartial investigation in the matter. They may obtain technical or any other support, if required, during investigation.

**16. Decision**

If an investigation leads the Chief Internal Vigilance Officer / Chairman of the Audit Committee, to conclude that an improper or unethical act has been committed, they shall recommend appropriate action against the _subject/s‘ to the management of the Bank. However, any disciplinary or corrective action initiated against the _subject‘ shall be as per extant service rules, applicable to him/her. In case of the _subject‘ being a director, **Chairman of the Audit Committee after investigation shall have power to refer the case to the Board of Directors for appropriated action against such „subject“**.

**17. Reporting to Audit Committee on Half-yearly Basis**

The Chief Internal Vigilance Officer shall submit a report to the Audit Committee on half yearly basis about all _protected disclosures‘ referred to him/her since the last report together with the results of investigation, if any.

**18. Retention of Documents**

All _protected disclosures‘ in writing or documented along with the findings of investigation relating thereto shall be retained by the Bank for a minimum period of seven years.

**19. Amendments**

The Bank reserves its right to amend or modify this Policy in whole or in part, at any time, however no such amendment or modification will be binding on its employees/ directors and specified third party stakeholders unless the same is properly notified.

**20. <u>Rewards for Whistle Blower</u>**. The management may at its sole discretion, consider rewarding the whistleblower (either by way appreciation/ acknowledgements or any other non-monetary/ monitory means) on case-to-case basis keeping in view the nature of the issue/s escalated.

**********

## Annexure "D" : Fraud Prevention Score Card[14] for Business Units and Other Operational Offices:

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

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

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

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

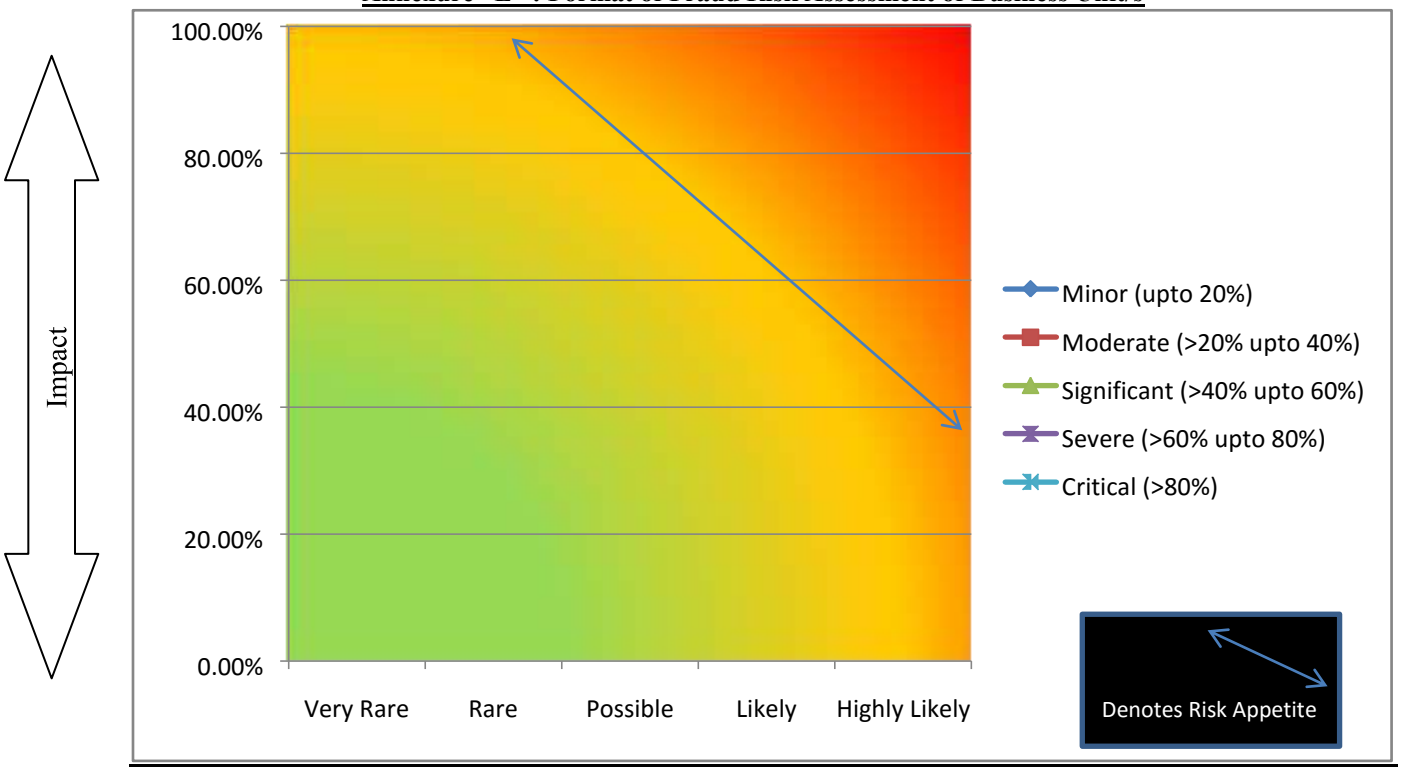
Each area, factor, or consideration scored either red or yellow should have a note associated with it that describes the action plan for bringing it to green on the next scorecard.

| S. No. | Fraud Prevention Area, Factor, or Consideration | Score | | Remarks / justification of the Score |
|---|---|---|---|---|
| | | Color | Numerical | |
| 1 | The business unit/ Office are committed to establish a zerotolerance environment with respect to fraud. | | | |
| 2 | The business unit/ Office displays the appropriate attitude regarding fraud prevention and encourages free and open communication regarding ethical behavior. | | | |
| 3 | Our Code of Organizational Conduct has specific provisions that address and prohibit inappropriate relationships whereby staff could use their positions for personal gain or other inappropriate purposes. The staff posted at the business unit / Office do not misuse their official position/s. | | | |
| 4 | We have done a rigorous fraud risk assessment using the related provisions of the subject Preventive Vigilance Framework and have taken specific actions to strengthen our prevention mechanisms as necessary. | | | |
| 5 | The staff posted at the Business unit/ Office is well aware of the latest trends of the fraud events in the banking industry and the fraud incidents that took place in the bank and information shared through various circulars. | | | |

[14] Each Red would entail a score of (minus 10.00), Yellow (minus 2.50) and Green (plus 10.00).

| | | | | |
|---|---|---|---|---|
| 6 | We have addressed the strengths and weaknesses of our internal control environment adequately and have taken specific steps to strengthen the internal control structure to help prevent the occurrences of fraud. | | | |
| 7 | The business unit / Office contains no unnecessary entities that might be used for inappropriate purposes or that might enable lessthan-arms-length transactions or relationships. | | | |
| 8 | We have assessed all business operations/ areas carefully and have taken proactive steps to ensure that they have fraud preventive controls in place to conform with the strictest legal standards and highest ethical principles as per the RBI/Bank directions on the subject from time to time. | | | |
| 9 | All the staff is well aware of the bank‘s whistleblower policy and | | | |
| | fraud hotline/email and the related procedures are known to all staff, vendors, contractors, and business partners. | | | |
| 10 | For any remaining third-party and related-party relationships, we have taken positive measures to ensure that such relationships do not allow opportunities for frauds to occur without detection. | | | |
| | **Overall Score (Also in Percentage).** | | | |

## Annexure "E" : Format of Fraud Risk Assessment of Business Unit/s




**Likelihood of Occurrence**

Each business unit will be required to assess major fraud-prone areas (illustrative list given in table below) of its business profile in the chart above or at least complete the table given below:

| S. No. | Fraud Prone Areas[15] | Impact | Likelihood of Occurrence | Remarks/ Justifications for the Impact |
|---|---|---|---|---|
| 1. | Illegal / irregular manipulation of records, documents, withdrawal of money | | | |
| 2. | Falsification of loan documents and/ or cases of impersonation | | | |
| 3. | Unauthorized credit facilities extended for reward or for illegal gratification | | | |
| 4. | Cheating & forgery on account of fake loan documents | | | |
| 5. | Unusual activities and transactions | | | |
| 6. | Cheque cloning | | | |
| 7. | Stealing / sharing of passwords | | | |
| 8. | Manipulations in any intermediary / parking accounts | | | |
| 9. | Inter-branch transactions in dormant accounts | | | |

[15] As stated above it is only an illustrative list. Each business unit Head to make proper due diligence of its own fraud risk vulnerability as per the business profile and other related aspects.

| | | | | |
|---|---|---|---|---|
| 10. | Non-KYC issues and anti-money laundering | | | |
| 11. | Opening accounts in fictitious names | | | |
| | | | | |
| | | | | |
| | | | | |

## Annexure "F" : Fraud Prevention Score Card[16] for Concerned Departments at Corporate Headquarters

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

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

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

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

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

| S. No. | Fraud Prevention Area, Factor, or Consideration | Score | | Remarks / justification of the Score |
|---|---|---|---|---|
| | | Color | Numerical | |
| 1 | Bank's organizational culture — tone at the top — is as strong as it can possibly be and establishes a zero-tolerance environment with respect to fraud. | | | |
| 2 | Bank's top management consistently displays the appropriate attitude regarding fraud prevention and encourages free and open communication regarding ethical behavior. | | | |
| 3 | Our Code of Conduct has specific provisions that address and prohibit inappropriate relationships whereby staff, members of our board or members of management could use their positions for personal gain or other inappropriate purposes. | | | |
| 4 | We have done a rigorous fraud risk assessment taken specific actions to strengthen our prevention mechanisms as necessary. | | | |
| 5 | We have assessed fraud risk for our organization adequately based on periodic reassessments of risk. | | | |
| 6 | We have addressed the strengths and weaknesses of our internal control environment adequately and have taken specific steps to strengthen the internal control structure to help prevent the occurrences of fraud. | | | |
| 7 | Our organizational structure contains no unnecessary entities that might be used for inappropriate purposes or that might enable lessthan-arms-length transactions or relationships. | | | |
| 8 | We have assessed all aspects of banking operations carefully and have taken proactive steps to ensure that they have fraud preventive controls in place to conform with the strictest legal standards and highest ethical principles. | | | |
| 9 | For any third-party and related-party relationships, we have taken positive measures to ensure that such relationships do not allow opportunities for frauds to occur without detection. | | | |

[16] Each Red would entail a score of (minus 10.00), Yellow (minus 2.50) and Green (plus 10.00).

| | | | | |
|---|---|---|---|---|
| 10 | We have assessed the alignment of authorities and responsibilities at all levels of organization management and are not aware of any misalignments that might represent vulnerabilities to fraud. | | | |
| 11 | Our audit committee is composed only of independent directors | | | |
| | and includes persons with financial accounting and reporting expertise. The audit committee has taken a very proactive posture with respect to fraud prevention. | | | |
| 12 | Our audit committee, that meets periodically, is proactively monitoring the implementation of fraud preventive mechanisms. | | | |
| 13 | The HRD department conducts background investigations with the specific objective of assuring that persons with inappropriate records or characters inconsistent with our corporate culture and ethics are identified and dealt with suitably as per extant Service Rules . | | | |
| 14 | The HRD department conducts background investigations with respect to promotions or transfers into positions of responsibility so that the persons with disputable charter are not posted in important positions and posts. | | | |
| 15 | All of our employees, vendors, contractors, and business partners have been made aware of our zero-tolerance policies related to fraud and are aware of the appropriate steps to take in the event that any evidence of possible fraud comes to their attention. | | | |
| 16 | We have a rigorous program for communicating our fraud prevention policies and procedures to all employees, vendors, contractors, and business partners. | | | |
| 17 | We have policies and procedures in place for authorization and approvals of certain types of transactions and for certain values of transactions to help prevent and detect the occurrences of fraud. | | | |
| 18 | Our performance measurement and evaluation process includes an element specifically addressing ethics and integrity as well as adherence to the Code of Organizational Conduct. | | | |
| 19 | All newly recruited staff is educated/ made aware about ethical code of conduct and fraud awareness and fraud prevention measures/ training. | | | |
| 20 | We have an effective whistleblower protection policy in vogue and its existence and procedures are known to all employees, vendors, contractors, and business partners. | | | |
| 21 | We review the above fraud preventive mechanisms on an ongoing basis and document these reviews as well as the communication with the audit committee/ Board regarding areas that need improvement. | | | |
| 22 | We have a fraud response plan in place and know how to respond if a fraud allegation is made. The fraud response plan considers:<br>• Who should perform the investigation?<br>• How the investigation should be performed?<br>• How to determine the remedial action.<br>• How to remedy control deficiencies identified.<br>• How to administer disciplinary action. | | | |
| | **Overall Score (Also in Percentage).** | | | |

## Annexure "G" : General Fraud-prone / Red-Flag Areas in the books of Bank"s Constituents to be Checked on Sample basis during Inspections by Manager Advances/ Branch Heads or Other Inspecting Officers of the Bank

| Asset Misappropriation | Modes through which It is Perpetrated |
|---|---|
| **Cash** | |
| i) Theft of cash | □ Stealing from petty cash. |
| | • Taking money from the till. |
| | • Skimming of cash before recording revenues or receivables (understating sales or receivables). |
| | • Stealing incoming cash or cheques through an account set up to look like a bona fide payee. |
| ii) False payment requests | Employee creating false payment instruction with forged signatures and submitting it for processing. |
| | • False email payment request together with hard copy printout with forged approval signature. |
| | • Taking advantage of the lack of time which typically occurs during book closing to get false invoices approved and paid. |
| | |
| **Cheque fraud** | Theft of company cheques. |
| | • Duplicating or counterfeiting of company cheques. |
| | • Tampering with company cheques (payee/amount). |
| | • Depositing a cheque into a third party account without authority. |
| | • Cheque kiting (a fraud scheme using two deposit accounts to withdraw money illegally from the bank). |
| | • Paying a cheque to the company knowing that insufficient funds are in the account to cover it. |
| | |
| **Billing schemes** | □ Over-billing customers. |
| | • Recording of false credits, rebates or refunds to customers. |
| | • Pay and return schemes (where an employee creates an overpayment to a supplier and pockets the subsequent refund). |
| | Using fictitious suppliers or shell companies for false billing. |
| | |
| **Misuse of accounts** | □ Wire/ online transfer fraud (fraudulent transfers into bank accounts). |
| | • Unrecorded sales or receivables. |
| | • Employee account fraud (where an employee is also a customer and the employee makes unauthorized adjustments to their accounts). |
| | • Writing false credit note to customers with details of an employee's personal bank account or of an account of a company controlled by the employee. |
| | • Stealing passwords to payment systems and inputting series of payments to own account. |
| | |
| **Non-cash** | |
| i) Inventory and fixed assets | □ Theft of inventory. |
| | • False write offs and other debits to inventory. |
| | • False sales of inventory. |
| | • Theft of fixed assets, including computers and other IT related assets. |
| | • Theft or abuse of proprietary or confidential information (customer information, intellectual property, pricing schedules, business plans etc). |
| | • Receiving free or below market value goods and services from suppliers. |
| | • Unauthorised private use of company property. |
| | • Employees trading for their own account |

| | |
|---|---|
| | |
| Procurement | Altering legitimate purchase orders. |
| | • Falsifying documents to obtain authorization for payment. |
| | • Forging signatures on payment authorizations. |
| | • Submitting for payment false invoices from fictitious or actual suppliers. |
| | • Improper changes to supplier payment terms or other supplier details. |
| | • Intercepting payments to suppliers. |
| | • Sending fictitious or duplicate invoices to suppliers. |

| | |
|---|---|
| | • Improper use of company credit cards. |
| | Marked up invoices from contracts awarded to supplier associated with an employee. |
| | • Sale of critical bid information, contract details or other sensitive information |
| | |
| Payroll | Fictitious (or ghost) employees on the payroll. |
| | • Falsifying work hours to achieve fraudulent overtime payments. |
| | • Abuse of commission schemes. |
| | • Improper changes in salary levels. |
| | • Abuse of holiday leave or time off entitlements. |
| | • Submitting inflated or false expense claims. |
| | • Adding private expenses to legitimate expense claims. |
| | • Applying for multiple reimbursements of the same expenses. |
| | • False workers' compensation claims. |
| | • Theft of employee contributions to benefit plans. |
| | |
| **Fraudulent statements** | |
| i) Financial : Improper revenue recognition | • Holding the books open after the end of the accounting period. |
| | • Inflation of sales figures which are credited out after the year end. |
| | • Backdating agreements. |
| | • Recording fictitious sales and shipping. |
| | • Improper classification of revenues. |
| | • Inappropriate estimates for returns, price adjustments and other concessions. |
| | • Manipulation of rebates. |
| | • Recognizing revenue on disputed claims against customers. |
| | • Recognizing income on products shipped for trial or evaluation purposes. |
| | • Improper recording of consignment or contingency sales. |
| | • Over/under estimating percentage of work completed on long-term contracts. |
| | • Incorrect inclusion of related party receivables. |
| | • Side letter agreements (agreements made outside formal contracts). |
| | • Round tripping (practice whereby two companies buy and sell the same amount of a commodity at the same price at the same time. The trading lacks economic substance and results in overstated revenues. |
| | • Bill and hold transactions (where the seller bills the customer for goods but does not ship the product until a later date). |
| | • Early delivery of product/services (eg partial shipments, soft sales, contracts with multiple deliverables, upfront fees). |
| | • Channel stuffing or trade loading (where a company inflates its sales figures by forcing more products through a distribution channel than the channel is capable of selling). |
| | |
| ii) Misstatement of assets, liabilities and/or expenses | • Fictitious fixed assets. |

| | |
|---|---|
| | • Overstating assets acquired through merger and acquisitions. |
| | • Improper capitalisation of expenses as fixed assets (software development, research and development, start up costs, interest costs, advertising costs). |
| | • Manipulation of fixed asset valuations. |
| | • Schemes involving inappropriate depreciation or amortisation. |
| | • Incorrect values attached to goodwill or other intangibles. |
| | • Fictitious investments. |
| | • Improper investment valuation (misclassification of investments, recording unrealised investments, declines in fair market value/overvaluation). |
| | • Fictitious bank accounts. |
| | • Inflating inventory quantity through inclusion of fictitious inventory. |
| | • Improper valuation of inventory. |
| | • Fraudulent or improper capitalisation of inventory. |
| | • Manipulation of inventory counts. |
| | • Accounts receivable schemes (eg creating fictitious receivables or artificially inflating the value of receivables). |
| | Misstatement of prepayments and accruals. |
| | • Understating loans and payables. |
| | • Fraudulent management estimates for provisions, reserves, foreign currency translation, impairment etc. |
| | • Off balance sheet items. |
| | • Delaying the recording of expenses to the next accounting period. |
| | |
| ii) Other accounting misstatements | Improper treatment of inter-company accounts. |
| | • Non clearance or improper clearance of suspense accounts. |
| | • Misrepresentation of suspense accounts for fraudulent activity. |
| | • Improper accounting for mergers, acquisitions, disposals and joint ventures. |
| | • Manipulation of assumptions used for determining fair value of share based payments. |
| | • Improper or inadequate disclosures. |
| | • Fictitious general ledger accounts. |
| | • Journal entry fraud (using accounting journal entries to fraudulently adjust financial statements). |
| | • Concealment of losses. |
| | |
| Non-financial | • Falsified employment credentials eg qualifications and references. |
| | • Other fraudulent internal or external documents. |
| | |
| **Corruption** | |
| i) Conflicts of interest | Kickbacks |
| | • Kickbacks to employees by a supplier in return for the supplier receiving favourable treatment. |
| | • Kickbacks to senior management in relation to the acquisition of a new business or disposal of part of the business. |
| | • Employee sells company owned property at less than market value to receive a kickback or to sell the property back to the company at a higher price in the future. |
| | Purchase of property at higher than market value in exchange for a kickback. |
| | • Preferential treatment of customers in return for a kickback. |
| | |
| ii) Personal interests | Collusion with customers and/or suppliers. |
| | • Favoring a supplier in which the employee has a financial interest. |

| | |
|---|---|
| | • Employee setting up and using own consultancy for personal gain (conflicts with the company‘s interests). |
| | • Employee hiring someone close to them over another more qualified applicant. |
| | • Transfer of knowledge to a competitor by an employee who intends to join the competitor‘s company. |
| | • Misrepresentation by insiders with regard to a corporate merger, acquisition or investment. |
| | • Insider trading (using business information not released to the public to gain profits from trading in the financial markets). |
| | |
| **Bribery and extortion** | |
| i)Bribery | Payment of agency/facilitation fees (or bribes) in order to secure a contract. |
| | • Authorizing orders to a particular supplier in return for bribes. |
| | • Giving and accepting payments to favour or not favour other commercial transactions or relationships. |
| | • Payments to government officials to obtain a benefit (e.g. customs officials, tax inspectors). |
| | • Anti-trust activities such as price fixing or bid rigging. |
| | • Illegal political contributions. |
| | |
| ii) Extortion | Offering to keep someone from harm in exchange for money or other consideration. |
| | • Blackmail – offering to keep information confidential in return for money or other consideration. |