Bangladesh Journal of Political Economy

Research Note

Vol. 31, No. 4, June 2016, pp. 513-532
Bangladesh Economic Association
(ISSN 2227-3182)

Financial Sector Development: Fraud Risk Management in Banks

Mohammad Ali*

Abstract: *The overall objective of this study is to acquire the practical knowledge about how banks and financial institutions are exposed to fraud and manages fraud risk in their institutions. The perpetrators are typically university educated and most fraudsters are aged between 36 and 55. As part of bank's governance structure, a fraud risk management program should be in place, including written policy for guidance of the Board of Directors and senior management regarding managing fraud risk. Fraud risk exposure should be assessed periodically by the bank to identify specific potential schemes and events that the bank needs to mitigate. It entails planning, identifying and evaluating fraud risk factors. Prevention techniques to avoid potential key fraud risk events should be established, where feasible, to mitigate possible impacts on the bank. Prevention techniques be related to sound ethical culture, fraud risk training and awareness, periodic fraud risk assessment, sound internal control system, reporting mechanisms and whistle blowing and pre-employment screening.*

1. Introduction

The term 'fraud' commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion. The legal definition varies from country to country. Fraud essentially involves using deception to dishonestly make a personal gain for oneself and/or create a loss for another.

Types of Fraud

- crimes by individuals against consumers, clients or other business people, e.g. misrepresentation of the quality of goods
- employee fraud against employers, e.g. payroll fraud; falsifying expense claims; thefts of cash, assets or intellectual property (IP); false accounting

* Mohammad Ali, Principal Officer, Risk Management Wing, Islami Bank Bangladesh Limited

- crimes by businesses against investors, consumers and employees, e.g. financial statement fraud; selling counterfeit goods as genuine ones; not paying over tax collected at source
- crimes against financial institutions, e.g. using lost and stolen credit cards; cheque frauds; fraudulent insurance claims
- crimes by individuals or businesses against government, e.g. grant fraud; tax evasion
- crimes by professional criminals against major organizations, e.g. major counterfeiting rings; mortgage frauds; identity fraud; money laundering
- e-crime by people using computers and technology to commit crimes, e.g. phishing; spamming; copyright crimes; hacking; social engineering frauds

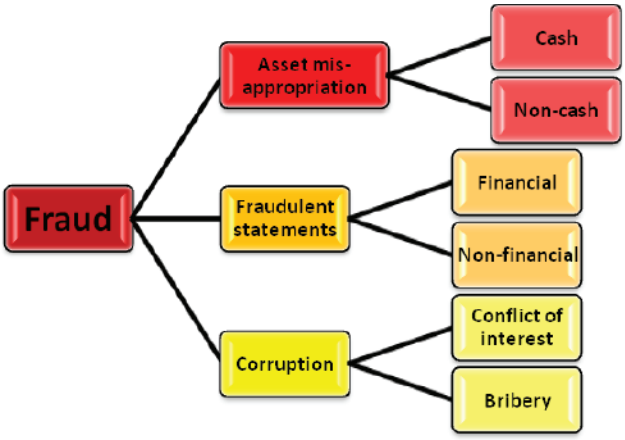


Figure: Types of Fraud

The impact of Fraud

- Reduced operational efficiency
- Loss of funds
- Bad press publicity
- Loss of trust
- Staff anxiety
- Investigation costs
- Confidentiality compromised

- Damage to credibility
- Strategic plans jeopardized
- Throwing good money after bad

2. Common Fraud & Forgeries

General Banking Port-folio:

√ Misappropriation of Branch cash from the Vault/Counter.

√ Misappropriation of cash by keeping less number of notes in the bundle.

√ Misappropriation of money by changing Cash position through cutting/overwriting etc.

√ Misappropriation of money by receiving cash from the depositors without depositing the same in the clients account as well as Cash Received Book.

√ By transferring Cash in other accounts by cutting/overwriting in the Branch's Books & Records.

√ Sometimes it is being done by showing false transfer of cash from one branch/bank to other Branch/Bank. Misappropriation of cash has been done directly by drawing cash from Feeding Branch. It is also being done by Receiving Cash from feeding branch & non-responding related IBDA for few days.

√ Misappropriation also done by not depositing the cash in clients A/c which has been received earlier and issuing false statement thereagainst.

√ By making false debit/credit voucher of Inter Branch/Other Banks transaction.

√ By making Payment of money against false issued PO/Security Receipt/TT/DD etc. without receiving cash thereagainst.

√ By duplicating clients signature/issuing duplicate cheque fraudulently & withdrawal of money from clients A/c- Instead of using the cheque requisition slip in the issued Cheque Book, Receiving Cheque Book against other application/form & withdrawal money from the client fraudulently.

√ Taking away cash from vault/safe using duplicate keys.

√ Unauthorized withdrawal of cash from the A/c by changing AOF & SS card.

- √ Misappropriation by changing the figures of instruments.
- √ Unauthorised withdrawal against fake DD/TT/IBCA etc.
- √ Misappropriation by non-depositing full/partial amount of commission in Banks A/c as received against issued DD/TT/PO/LC/BG etc.
- √ Misappropriation of the Income/ Service Charges, Commission etc.
- √ Misappropriation by excess credit of profit on deposits.
- √ Recording of excess expenses to the expenses genuinely incurred.
- √ Forging of signatures and documents crediting customers deposits to fictitious names, forging customers signatures on cheques and notes.
- √ Debiting the customer's A/c with unauthorised entry.
- √ Release of the documents attached to drafts held for collection without recovery full payment.
- √ Payment from dormant account to wrong person/unauthorised withdrawal from dormant Account.
- √ Changing the amount of DD and en-cashing the draft.
- √ Charging the same cheque twice to the customer.
- √ Misappropriation of cash by keeping notes of less value in the bundles of higher value.
- √ Misappropriation of cash by replacing original vouchers with fake ones.
- √ Misappropriation of cash through false remittances.
- √ Misappropriation of cash by changing/altering the original figure in the cheques.
- √ Misappropriation of cash from different types of Bank's A/Cs by creating anomalies/fake vouchers.

Investment Portfolio

- √ Defalcation of cash by allowing fictitious investment.
- √ Defalcation of cash by allowing investment against fake collaterals.
- √ Defalcation of cash by allowing investment against fake share certificates as collateral security.
- √ Allowing investment against fake Delivery Orders
- √ Allowing investment/extending investment in the name of fictitious persons/firms

- √ Allowing investment exceeding ZO/HO sanctioned limit.
- √ Allowing investment by the branch incumbent without any collateral security.
- √ Allowing investment showing inflated rate of purchased goods etc.
- √ Allowing CC/LIM against less/nil pledge of goods/stocks.
- √ Allowing investment against inflated value of collaterals.
- √ Misappropriation of money by creating unusual/false investments.
- √ Fraudulently using the securities of the customers.
- √ Exercising powers beyond those authorised, for example, making unauthorised investment, release of collateral security without getting the investment account squared, making investment on worthless security.

Foreign Exchange Portfolio

- √ Allowing L/C facilities to fictitious importer.
- √ Payment of F/C against fake export L/C by opening Back to Back L/C.
- √ Remittance of Foreign Currency through over invoicing.
- √ Remittance of Foreign Currency through false/fake document.
- √ Remittance of Foreign Currency through fraudulent means (issuance of Cash/FC/TC to the false tourist/students/patients).
- √ Release of Import documents without recovery of full payment.
- √ Misappropriation done by debiting Head Office, International Banking Wing at enhanced rate of exchange & showing credit to other account.
- √ Opening of L/C by violating discretionary power/exceeding Head Office/Zonal Office limit
- √ Opening L/C without realising cash security, L/C opening commission, L/C amendment commission etc.
- √ Endorsement of copy documents without receiving payment there against.
- √ Delivering documents without receiving payment/creation of MPI for clearance of the consignment by the client without securing the bank.
- √ Allowing clearance of the goods under MPI through the client/client's C & F agent instead of banks approved C & F agent.
- √ Holding cash security held against L/C which has been released for adjustment of the client's other liability.

- √ Adjusting the cost of F/C (Value of the IBDA's) by debiting the WES Fund Purchase A/c. Instead of realising the Bank's dues against the bills from the client either in cash or by creating investment.
- √ Creation of MPI for payment of custom duties only keeping the other related liabilities under Mura WES L/C & Mura WES Bills A/c.
- √ Making advance payment against import.
- √ Effecting export making under invoicing.
- √ Settling Payment by local currency or by goods without remitting equivalent. F.C. to the country.
- √ Depositing/paying of F. C. without having adequate coverage from Nostro A/c.
- √ Encashment of fake Instrument DD/TT/TC/MT etc.
- √ Issuance/Endorsement of Cash F.C., DD, TC beyond celing or violating guidelines of B.B./F.E. circulars.
- √ Endorsement of F.C. (Cash/TC) to fake personnel or in fake passports.
- √ Encashment of F.C. instrument through misdeclaration:
- √ Indenting commission received in personal name declaring normal remittance to escape from relevant Tax payment
- √ FC paid through advance realisation of proceeds without effecting export.
- √ Export documents negotiated & purchased keeping major discrepancies/obtaining fake document.
- √ Donation, subscription against organisations/firms realised in personal name.
- √ Illegal disposal of custom bonded imported goods
- √ Pre-shipment financed against fake export order or without having raw materials
- √ Wilful creation of stock lot to sell the goods at discount rate (predetermined)

IT Portfolio

- √ Non checking/cross-checking of daily corrected and reversed transaction list by the Manager/2nd Officer/Authorized Officer;
- √ Non checking of daily transaction lists with vouchers/cheques/instruments by authorized officials of the Branch;

- √ General Banking, Investment, Foreign exchange & Remittance related transaction lists and account opening data at the end of the day's transactions are not checked & preserved by the responsible official(s) other than the operator properly as instructed by ICTD;
- √ Running day end process without proper checking of the daily transaction list which results the mistakes made by the users/operators to be carried forward or to be retained undetected;
- √ Symbolical user names are used instead of the actual user names, privacy of user name & password is not maintained;
- √ Withdrawal limit of operators are not set by the supervisors;
- √ Effective Rate of Return is not inserted and re-fixed/changed from time to time as instructed by different circulars from time to time which may cause leakage of investment profit.

The following precautionary measures may be taken to avoid the above stated frauds and forgeries:

- o Strict adherence to the rules, regulations, guidelines and instructions issued from time to time by the competent authority
- o Close supervision, monitoring and evaluation
- o Maintenance of books of accounts, registers etc. properly and regularly
- o Counter checking of books/registers
- o Conducting of periodical and surprise inspection
- o Rotation of officials through transfer/posting at regular intervals
- o Initiation of administrative and disciplinary actions against the delinquent staffs and officials
- o Awarding punishment to the officials involved with irregularities, mal practices and corruptions
- o Developing the knowledge & skill of the employees by training, regular study circular

3. Why Fraud is committed ?

There is relationship among following factors for committing frauds:

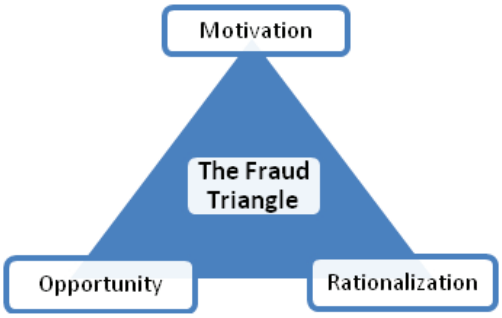


Figure: Fraud Triangle

Opportunity:

Fraud is more likely in banks where there is a weak internal control system, little likelihood of detection, or unclear policies .

Motivation:

Greed continues to be the main cause of fraud, other causes included problems from debts and gambling .

Rationalization :

- necessary – when done for the business
- harmless – because the victim is large enough
- justified – because 'the victim deserved it'

Who commits Fraud?

In 2010, KPMG carried out research on the Profile of a Fraudster (KPMG survey), using details of fraud cases in Europe, India, the Middle East and South Africa.

- perpetrators are typically university educated
- most fraudsters are aged between 36 and 55
- the majority of frauds are committed by men
- median losses caused by men are twice as great as those caused by women
- a high percentage of frauds are committed by senior management (including owners and executives)
- losses caused by managers are generally more than double those caused by employees
- average losses caused by owners and executives are nearly 12 times

those of employees

- longer term employees tend to commit much larger frauds
- fraudsters most often work in the finance or operations

4. Fraud Detection – Indicators

- Business risk
- Cultural issues
- Management issues
- Employee issues
- Process issues
- Transaction issues
- Financial Risk
- Environment Risk
- IT & Data Risk
- Fraud alerts

Fraud Detection - Business risk

- Cultural issues
  - Absence of an anti-fraud policy and culture.
  - Failure of management to implement a sound system of internal control and/or to demonstrate commitment to it at all times.
- Management issues
  - Lack of financial management expertise and professionalism in key accounting principles, review of judgments made in management reports and the review of significant cost estimates.
  - A history of legal or regulatory violations within the organization and/or claims alleging such violations.
  - Strained relationships within the organization between management and internal or external auditors.
  - Lack of management supervision of staff.
  - Lack of management control of responsibility, authorities, delegation
  - Bonus schemes linked to ambitious targets or directly to financial

results.

- Employee issues
  - Inadequate recruitment processes and absence of screening.
  - Unusually close relationships – internal and external.
  - Potential or actual labor force reductions or redundancies.
  - Dissatisfied employees who have access to desirable assets.
  - Unusual staff behavior patterns.
  - Personal financial pressures on key staff.
  - Low salary levels of key staff.
  - Poor dissemination of internal controls.
  - Employees working unsocial hours unsupervised.
  - Employees not taking annual leave requirements.
  - Unwillingness to share duties.
- Process issues
  - Lack of job segregation and independent checking of key transactions.
  - Lack of identification of the asset.
  - Poor management accountability and reporting systems.
  - Poor physical security of assets.
  - Poor access controls to physical assets and IT security systems.
  - Lack of and/or inadequacy of internal controls.
  - Poor documentation of internal controls.
- Transaction issues
  - Poor documentary support for specific transactions
  - Large cash transactions.
  - Susceptibility of assets to misappropriation.

Fraud Detection – Financial risk

- Management compensation highly dependent on meeting aggressive performance targets.
- Significant pressures on management to obtain additional finance.

- Complex transactions.
- Use of complex financial products.
- Complex legal ownership and/or organizational structures.
- Rapid changes in profitability.

Fraud Detection – Environment risk

- The introduction of new accounting or other regulatory requirements, including health and safety or environmental legislation, which could significantly alter reported results.
- Highly competitive market conditions and decreasing profitability levels within the organization.
- The organization operating in a declining business sector and/or facing prospects of business failure.
- Rapid technological changes which may increase potential for product obsolescence.
- Significant changes in customer demand.

Fraud Detection – IT & Data risk

- Unauthorized access to systems by employees or external attackers.
- The wealth of malicious codes and tools available to attackers.
- Rapid changes in information technology.
- Users not adopting good computer security practices, e.g. sharing or displaying passwords.
- Unauthorized electronic transfer of funds or other assets.
- Manipulation of programs or computer records to disguise the details of a transaction.
- Compromised business information.
- Breaches in data security and privacy.
- Sensitive data being stolen leaked or lost.

Fraud Detection – Fraud alerts

- Anonymous emails/letters/telephone calls.
- Emails sent at unusual times, with unnecessary attachments, or to unusual destinations.
- Discrepancy between earnings and lifestyle.

- Unusual, irrational, or inconsistent behavior.
- Alteration of documents and records.
- Extensive use of correction fluid and unusual erasures.
- Photocopies of documents in place of originals.
- Rubber Stamp signatures instead of originals.
- Signature or handwriting discrepancies.
- Missing approvals or authorization signatures.
- Transactions initiated without the appropriate authority.
- Subsidiary ledgers, which do not reconcile with control accounts.
- Extensive use of 'suspense' accounts.
- Inappropriate or unusual journal entries.
- Confirmation letters not returned.
- Supplies purchased in excess of need.
- Higher than average number of failed login attempts.
- Systems being accessed outside of normal work hours or from outside the normal work area.
- Controls or audit logs being switched off.

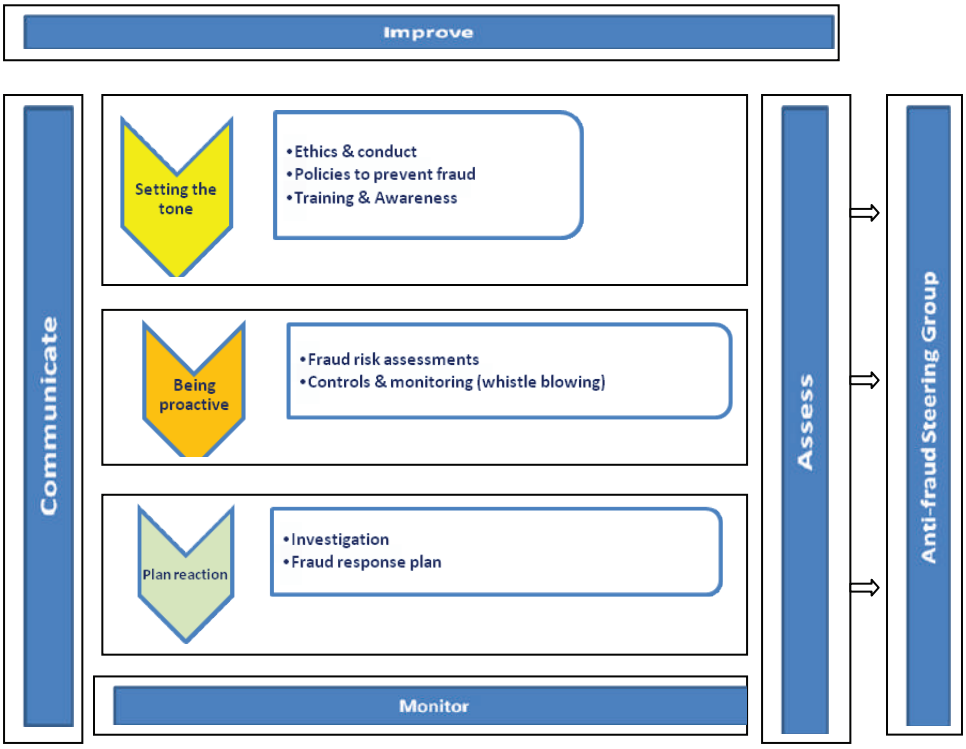
Fraud Risk Management – Programme

- As part of bank's governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding managing fraud risk.
- Roles & Responsibilities:
    - Board of Director's
    - Board audit committee
    - Management
    - Staff
- The following persons of bank or organisations should be involved in the Anti-fraud steering group:
    - CEO/ MD
    - Chief Risk Officer

- CFO
- Head of IT
- Head of Legal affairs Division
- Head of HR
- Heads of Branches Control Division

- The followings should be oversighting the Anti-fraud steering group:
  - Internal audit
  - The Board Audit Committee
  - The Board

Diagram of Fraud Risk Program:



Fraud Assessment Procedure

Fraud risk exposure should be assessed periodically by the bank to identify specific potential schemes and events that the bank needs to mitigate.

1. Planning
2. Identify and evaluate fraud risk factors

3. Identify possible fraud
4. Prioritize identified fraud risks
5. Evaluate mitigating controls
6. Risk treatment

1. Planning

Management should plan by taking responsibility which will be implemented through the Anti-Fraud Steering Group and should:

- ≥ Focus on high-risk areas and wide in scope
- ≥ Develop skill set through training or appoint specialists
- ≥ Ensure all relevant parts/people of the bank are involved
- ≥ Be systematic & recurring

2. Identify & evaluate fraud risk factors

Identify fraud risk factors at the entity level, significant locations, significant accounts and business process level. Use the Fraud Triangle to initiate thinking and take into account scope for management override of controls

3. Identify possible fraud

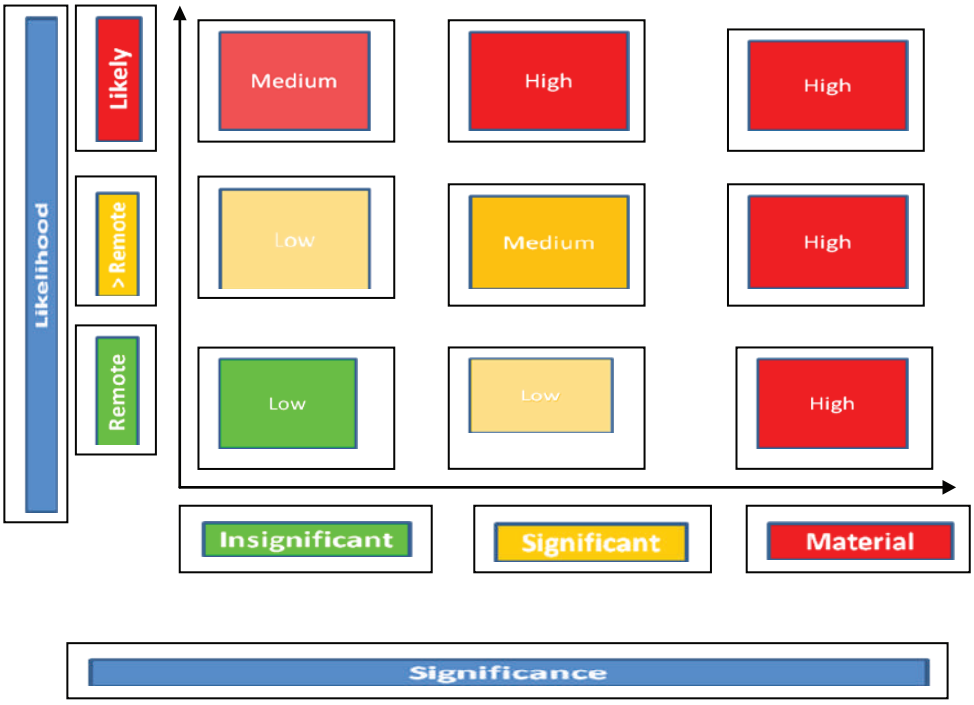
- ≥ For each identified fraud risk factor, identify the account balances and potential errors that may be affected and assess the fraud risks.
- ≥ Identify possible fraud risks and schemes.
- ≥ For each fraud scheme, identify internal and external parties who could be involved with reference to incentives / pressure, opportunities, attitudes & rationalizations.
- ≥ Identify fraud risks and determine if the fraud risks are pervasive or specific. Brainstorm specific fraud schemes that could result from the specific risks identified.

4. Prioritise identified fraud risk

Prioritize Identified Fraud Risks

a. Likelihood
b. Significance

Consider Inherent Risk Rating (IRR) based on likelihood & significance as follows:



5. Evaluate mitigating controls

- ≥ Link fraud schemes to mitigating controls. Assess whether each mapped or linked control activity is preventative or detective in nature.
  - ❄ Preventative controls are designed to mitigate specific fraud risks and can deter frauds from occurring
  - ❄ Detective control activities are designed to identify fraud if it occurs. Detective controls can also be used as a monitoring activity to assess the effectiveness of antifraud controls and may provide additional evidence of the effectiveness of antifraud programs and controls.
- ≥ Evaluate the effectiveness of controls to determine if they sufficiently mitigate the risk of the identified fraud schemes (control gap analysis).
- ≥ Special consideration should be given to the risk of override of controls by management
- ≥ Evaluate controls to determine if they sufficiently mitigate the identified fraud risks and schemes or if additional emphasis should be placed on existing controls or new controls are required.

≥ Consider both the design and the implementation of the control in mitigating the fraud risk

CONTROL RISK RATING as :

√ High

√ Medium

√ Low

A **"High"** rating would indicate immediate action is required and that item should be included in a fraud risk action plan.

A **"Medium"** rating would indicate that attention is required to the fraud risk and control and that item may be included in a fraud risk action plan, depending on the control effectiveness rating.

A **"Low"** rating would indicate that the item should be factored into ongoing monitoring plans.

6. Risk Treatment

Once the risks have been identified and assessed, strategies to deal with each risk identified can be developed by line management, with guidance from the anti-fraud steering committee. Strategies:

a. risk retention

b. risk avoidance

c. risk reduction

d. risk transfer

Before strategies are developed, it is necessary to establish the risk appetite of the bank. Risk appetite is the level of risk that the bank is prepared to accept and this should be determined by the board.

The appetite for risk will influence the strategies to be developed for managing risk. It is worth noting that a board's risk appetite may vary for different types of risk and over time.

Fraud Prevention

Prevention techniques to avoid potential key fraud risk events should be established, where feasible, to mitigate possible impacts on the bank.

- Developing a sound ethical culture
- Fraud risk training and awareness
- Periodic fraud risk assessment (already covered in detail)

- Sound internal control system (part of overall risk management strategy)
- Reporting mechanisms and whistle blowing
- Pre-employment screening

Fraud Prevention – Culture

- Attitudes within a bank often lay the foundation for a high or low fraud risk environment. Where minor unethical practices may be overlooked (e.g. petty theft, expenses frauds), larger frauds committed by higher levels of management may also be treated in a similar lenient fashion. In this environment there may be a risk of total collapse of the bank either through a single catastrophic fraud or through the combined weight of many smaller frauds.
- The definition of good ethical practice is not simple. Ideas differ across cultural and national boundaries and change over time. But corporate ethics statements need not be lengthy to be effective.
- A mission statement that refers to quality or, more unusually, to ethics and defines how the bank wants to be regarded externally
- Clear policy statements on business ethics and anti-fraud, with explanations about acceptable behavior in risk prone circumstances

Fraud Prevention – Training

- When a major fraud occurs people who were close to it are shocked that they were unaware of what was happening.
- Therefore, it is important to raise awareness through a formal education and training program as part of the overall risk management strategy.
- Particular attention should be paid to those managers and staff operating in high risk areas.

Fraud Prevention – Whistle blowing

- Establishing effective reporting mechanisms is one of the key elements of a fraud prevention program and can have a positive impact on fraud detection.
- Many frauds are known or suspected by people who are not involved. The challenge for management is to encourage these ‘innocent’ people to speak out.
- In this area there are many conflicting emotions influencing the potential ‘whistleblower’:

- working group/family loyalties
- disinterest/sneaking admiration
- fear of consequences
- suspicion rather than proof
- A confidential 24/7 hotline is said to be one of the best methods for reporting fraud.

Fraud Prevention – Staff Screening

- Pre-employment screening is the process of verifying the qualifications, suitability and experience of a potential candidate for employment.
- Techniques used include confirmation of educational and professional qualifications, verification of employment background, criminal history searches, and credit checks.
- Screening applicants should reduce the likelihood of people with a history of dishonest or fraudulent behavior being given a role within the bank, and is therefore an important fraud prevention procedure.
- Research has also shown that employers who conduct pre-employment screening experience fewer cases of fraud.

Response to the detected fraud

Reasonable steps for responding to detected or suspected instances of fraud include:

- clear reporting mechanisms
- a thorough investigation
- disciplining of the individuals responsible (internal, civil and/or criminal)
- recovery of stolen funds or property
- modification of the anti-fraud strategy

- The fraud response plan is a formal means of setting down clearly the arrangements which are in place for dealing with detected or suspected cases of fraud.

The response procedure should include:

- Reporting suspicions
- Establish an investigation team
  - Objectives

- reporting procedures
- Responsibilities
- Powers
- control

- Formulate a response
  - in accordance with bank policy
  - The investigation
- Preservation of evidence/ Physical evidence/ Electronic evidence
- Interviews (general)/ Statements from witnesses/ Statements from suspects

Administration of Fraud Risk Management Policy

The Internal Control Committee (under Internal Control & Compliance Risk) may ensure the effectiveness of the Policy. Revisions to this policy will be submitted to the Risk Management Committee of the Board for review and approval. The policy will be reviewed annually and revised as needed.

References

1. Mamun Rashid, "Combating fraud in banks" 18 September 2013 in The Daily Financial Express

2. The Financial Express, "Transforming big data into big business value highlighted", 04 Nov, 2014.