Manual of Combatting Embezzlement & Financial Fraud & Control Guidelines

2008
Contents

1 Preamble 5 1
2 Introduction 6 2
2-1 Overview 6 2
2-2 Definition of Fraud 7 2-2
2-3 Fraud & Money- Laundering 9 3-2
2-4 Examples of Fraud 9 4-2
2-5 Technology Role 10 5-2
2-6 SAMA’s Circulars & Supporting Guidelines 11 6-2

3- Plan for Combating and Preventing Fraud 13 3
3-1 Introduction 13 1-3
3-2 First Basic Condition: the Strategy of Fraud Combating and Control Policy: 14 2-3
3-2-1 Introduction 14 1-2-3
3-2-2 Guidelines 14 2-2-3
3-3 Second Basic Condition: Regulatory Framework and Responsibility 16 3-3
3-3-1 Introduction 16 1-3-3
3-3-2 Guidelines 16 2-3-3
3-3-2-1 Management Responsibilities 16 1-2-3-3
3-3-2-2 Fraud Control Committee 17 2-2-3-3
3-3-2-3 Fraud Investigation Unit 18 3-2-3-3
3-3-2-4 Combating and Detection 20 4-2-3-3
3-3-2-5 Employees’ Responsibilities 21 5-2-3-3
3-4 Third Basic Condition: Assessment of Fraud Risk 22 4-3
3-4-1 Introduction 22 1-4-3
3-4-2 Guidelines 22 2-4-3

جدول المحتويات 1

تمهيد 1

مقامة 2

لمحة عامة 1-2

تعريف الاحتيال 2-2

الاحتيال وغسل الأموال 3-2

عينة من أمثلة الاحتيال 4-2

دور التقنية 5-2

تعاميم مؤسسة النقد العربي السعودي والخطوات الإرشادية للمساعدة 6-2

خطة مكافحة ومنع الاحتيال 3

شرح الأساسي الأول: استراتيجيّة 2-3

مكافحة الاحتيال وسياسة الرقابة 1-2-3

الإرشادات 2-2-3

شرح الأساسي الثاني: الإطار التنظيمي وهيكلية المسؤولية 3-3

المؤسسات الإدارية 1-2-3-3

لجنة مراقبة الاحتيال 2-2-3-3

وحدة التحقق بشأن الاحتيال 3-2-3-3

الاحتيال والكشف 4-2-3-3

مسؤوليات الموظفين 5-2-3-3

شرح الأساسي الثالث: تقييم خطر الاحتيال 4-3

الإرشادات 1-4-3

الإرشادات 2-4-3
3-4-2-1  Assessment Process of Fraud Risks  23  23  
3-5  Fourth Basic Condition: Promoting Awareness of Fraud  24  24  
3-5-1  Introduction  24  24  
3-5-2  Guidelines  24  24  
3-5-2-1  Employee's Awareness  24  24  
3-5-2-2  Promotion of Customer's Awareness  26  26  
3-5-2-3  Promoting Awareness of Concerned Parties  26  26  
3-6  Fifth Basic Condition: Internal Control Procedures  26  26  
3-6-1  Introduction  26  26  
3-6-2  Guidelines  28  28  
3-6-2-1  Main Principles of Effective Internal Control  29  29  
3-6-2-2  Practices of Personnel  30  30  
3-6-2-3  Separation of Duties  32  32  
3-6-2-4  Dual Control  32  32  
3-6-2-5  The Policy of Gifts  33  33  
3-6-2-6  Dormant Accounts  33  33  
3-6-2-7  Cash Handling (Delivery and Taking over)  34  34  
3-6-2-8  Limits of Withdrawals  34  34  
3-6-2-9  Supervision of the Trading Room  34  34  
3-6-2-10  Conflict of Interests Management  36  36  
3-6-2-11  Protection of Intellectual Property  38  38  
3-6-2-12  Information Systems Security  39  39  
3-6-2-13  Fraudulent Invitations  40  40  
3-7  Sixth Basic Condition: Follow-up Process  41  41  
3-7-1  Introduction  41  41  
3-7-2  Guidelines  42  42  
3-7-2-1  Internal Follow-up  42  42  
3-7-2-2  External Follow-up  44  44  
3-7-2-3  The Policy of Monitoring, Control and 

1-2-4-3  عملية تقييم مخاطر الاحتيال  
5-3  الشرط الأساسي الرابع: نشر الوعي بشأن الاحتيال  
1-5-3  مقدمة  
2-5-3  الإرشادات  
1-2-5-3  وعي الموظف  
2-2-5-3  توعية العميل  
3-2-5-3  تو única الأطراف ذات العلاقة

3-6-3  الشرط الأساسي الخامس: إجراءات الرقابة الداخلية  
1-6-3  مقدمة  
2-6-3  الإرشادات  
1-2-6-3  المبادئ الرئيسيّة للرقابة الداخلية الفاعلة

2-2-6-3  ممارسات التوظيف  
3-2-6-3  فصل الواجبات  
4-2-6-3  الرقابة المزدوجة  
5-2-6-3  سياسة منع الهدايا  
6-2-6-3  الحسابات الرائدة

7-2-6-3  مناولة النقد (تسليم واستلام)

8-2-6-3  الحدود  
9-2-6-3  الإشراف على غرفة المتابعة  
10-2-6-3  إدارة تضارب المصالح  
11-2-6-3  حماية الملكية الأدبية  
12-2-6-3  أمن أنظمة المعلومات  
13-2-6-3  الدعوات الاحترازية

7-3  الشرط الأساسي السادس: عملية المتابعة  
1-7-3  مقدمة  
2-7-3  الإرشادات  
1-2-7-3  المتابعة الداخلية  
2-2-7-3  المتابعة الخارجية

3-2-7-3  سياسة متابعة مراقبة الاحتيال ومكافحته.
Combat of Fraud

3-8 Seventh Basic Condition: System of Notification of Fraud
3-8-1 Introduction
3-8-2 Guidelines
3-8-2-1 Channels for Notification
3-8-2-2 Protection of Notification
3-8-2-3 External Notification
3-8-2-4 Receiving Notification Reports from Customers and the Public

3-9 Eighth Basic Condition: Investigation Standards
3-9-1 Introduction
3-9-2 Guidelines
3-9-2-1 Receiving a Notification of Alleged Fraud
3-9-2-2 Initial Evaluation
3-9-2-3 Updating Case Reports
3-9-2-4 Application of the Investigation Plan
3-9-2-5 Evidence Protection
3-9-2-6 Recovery of the Proceeds of Fraud

3-10 Ninth Basic Condition: Code of Conduct and Disciplinary Measures
3-10-2 Introduction
3-10-2-1 Code of Conduct
3-10-2-2 Disciplinary Standards
3-10-2-3 Standards Applicable to Outsourcing
Preamble

This manual includes general guidelines that should be taken into account upon designing or evaluating the policy related to preventing and combating fraud in the commercial banks operating in the Kingdom of Saudi Arabia. These guidelines are complementary to the previous ones issued by SAMA with regard to combating fraud; yet they are broader in scope and include controls that aim at combating embezzlement and financial fraud. Accordingly, the manual’s title has been changed to reflect this trend.

SAMA has prepared this manual to help banks’ managers and senior officials in assessing fraud risks in the banks and providing methods of how to encounter such operations through a general strategy that would fit each bank individually for combating and preventing fraud. These controls are principally based on nine basic conditions to set an effective strategy to combat, detect and control fraud. Each condition has a brief and general introduction followed by specific guidelines which aim at helping banks in applying these controls.

To cope with the development of practices followed to combat and prevent fraud acts, these guidelines will be updated from time to time.

In general, the guidelines aim at providing a practical manual for self-assessment by banks to apply a comprehensive strategy to combat fraud and serve as a draft project to be guided by. The manual should be used along with the above-mentioned SAMA’s guidelines and other relevant circulars. The manual is important to develop an integrated program to combat and control fraud acts so as to be among the tasks of the bank management of comprehensive operational risks and operation risks and also among the tasks of the bank’s internal control system.

The success of the controls for combating and preventing fraud basically depends on the extent of commitment by the bank’s board of directors and executive management to implement such controls. It also requires choosing an appropriate timing and the provision of necessary financial and human resources. To apply the process for combating fraud successfully, the management shall not only exercise the role of supervision and leadership but it must also set a good example in applying the best ethical standards and suitable professional conduct. Thus, these guidelines are straightly directed to the banks’ BODs and senior officials in addition to different functional groups, committees and individuals carrying out specific tasks related to the strategy of combating and controlling fraud acts.
Fraud is one of the challenges facing banking and financial institutions as it hinders performance, causes depletion of money and scarce resources and hurts the institution's reputation and its competitiveness. The damage may take several forms other than the financial loss itself no matter how heavy it is. The largest damage may be that which seriously affects the institution's performance, reputation, credibility, market's and public's confidence in it, and eventually, results in its exposure to various risks.

Fraud is a big problem which is not limited to a particular private financial, industrial or services institutions. Moreover it can adopt with changes which may arise in any sector. In spite of internal audit, control and investigation mechanisms and independent external auditors' conditions and professional conduct rules, the occurrence of fraud continues.

It is often difficult, and in most cases impossible, to recover the funds wasted due to fraudulent transactions. Thus the programs for combating and controlling fraud acts are much more cost effective than attempts to recover embezzled funds.

Although a number of banks resort to insurance to protect themselves from operational risks resulting from incidents such as fraud and embezzlement acts by their employees, yet they can not rely totally on insurance as a way for reducing operational risks. Delay in payment and challenges to contractual conditions prove that insurance does not provide an ideal coverage. In addition negative results of claims related to fraud will lead to an increase in insurance premiums, especially when market forces tend to raise insurance premiums even for banks with "clean records".

As for statutory capital adequacy recommended by Basel Committee for operational risks, banks will be required in future to allocate statutory reserves of their capital for operational risks. Banks with bad records in combating fraud will find that their financial resources will be affected negatively due to an increase in their capital reserves, apart from incurring direct financial losses and increasing insurance premiums.

Due to the rapid technological advancement and spread of organized crimes worldwide, it is necessary to review such strategy regularly and update it to cope with new risks and techniques used.
2-2 Definition of Fraud

Fraud is simply defined as any act involving deceit to obtain a direct or indirect financial benefit by the perpetrator or by others with his help, causing a loss to the deceived party. The actual loss of banks due to fraud is usually connected with liquid assets, such as cash and securities. Fraud is not necessarily limited to obtaining cash money and tangible benefits. Fraud definition as stated in the dictionary is "a deliberate distortion of a fact to entice someone to waive something valuable or a legal right ". This definition includes a financial gain in addition to other benefits, such as the right to have access to or obtain information by deceit or any other dishonest conduct.

Whether the loss is material or related to an intangible benefit such as intellectual property rights, fraud usually involves a loss to the bank, its shareholders or customers and an attempt to hide this loss.

The basic test of fraud may include the following questions:
- Has fraud been committed against the firm?
- Is the action illegal?
- Has such action resulted in financial benefits in favor of an undeserving person?
- Has there been an attempt to commit any of the acts as mentioned above?

There must be a differentiation between "an internal" fraud inside the bank and "an external" fraud outside the bank. Studies conducted on international institutions often indicate that fraud is always committed by the banks' employees with or without help from external partners. They are usually motivated by seizing opportunities, avidity, revenge, the need for spot cash to raise their standard of living, due to personal financial trouble, dissatisfaction, lack of allegiance, pressure of family needs or the need to repay debts.

Fraud cases in most countries of the world are similar in banks; they result from employees' fraudulent actions. Money embezzlement is the most common fraud act, especially embezzlement of funds and traveler's checks from branches and ATMs. It should be noted that the amounts gained by money embezzlement are always small. On the other hand, fraud acts via electronic payments or

by fraudsters. These guidelines aim at helping senior officials to carry out this task.
transfers may be small in number; yet they usually involve great financial losses.

It is well known historically that most fraud acts in banks are committed by all levels of employees working in these banks. Therefore any strategy aimed at combating fraud must mainly focus on what is called "Business Location" fraud.

At the same time, the concept of fraud should not disregard external fraud, referred to as fraud by customers. External fraud is committed by persons outside the bank (usually professional criminals) often with the help of persons inside the bank. Thus, to understand fraud correctly, we must understand that fraud acts are committed by persons who are trustworthy. External fraud is committed by persons who are trustworthy. At some point, it is likely that the fraudster takes a long time before discovering fraud, and why when the perpetrator is caught his colleagues are trustworthy. This explains why it often happens that the crime or the criminal source of money can not be traced.
2-4 Examples of Fraud

There are several examples of banking fraud such as the following:

- Embezzling cash money and other precious assets.
- Counterfeiting or distorting documents including job applications, bills, checks, eligibility or qualification certificates, identification documents, ATM or credit cards.
- Forging signatures and stamps.
- Forging cash money.
- Changing one or all check components.
- Stealing ATM or credit cards and using them fraudulently.
- Entering inappropriate directions and data in PCs.
- Misusing accessible information and divulging it illegally.
- Paying or transfer of money to illusory customers, employees or sellers.
- Taking bribes, gifts or secret commissions to award a contract; overlook non-compliance with obligations or to provide benefits including accessing confidential information.
- Obtaining through fraud documents or benefits that a receiver has no right to obtain.

2-5 Technology Role

Modern technology in the field of banking business has proven to be a double-edged weapon. On the one hand, efforts in combating fraud have obviously made use of modern technology. The transformation from the circulation of money into electronic transfer of funds has reduced the risks of money embezzlement due to a decrease in cash holding. The development of methods and equipment to detect fraud has been made by the dint of advanced technology.

On the other hand, fraudsters are skilled in suing the latest modern technologies to strengthen their capabilities. It might be said that fraud has further been facilitated by the wide spread of cheap and easily obtained PCs and other relevant technologies of high capabilities. The current documents' technologies, such as scanners, laser printers, different Xerox copying machines and programs, have allowed the commitment of forgery acts that are difficult to be detected. The simple methods of forging checks in the past have now been replaced.

included in theses guidelines though some measures to combat fraud as stated in this document may be parallel to the previously mentioned efforts that aim at combating money-laundering and terrorism financing.

استنادًاً وفقًاً لمقدمة الاقتراعات عن هذه الإرشادات مع أن بعض التدابير مثيرة للإحالة للمرة، هناك قد تجدر كما ورد سابقاً تطبيقًاً ملحواناً في الجهود الرامية إلى مكافحة عمل الأمور وتمويل الإرهاب.

4-2 عينة من عمليات الاحتيال:

هناك عدة أمثلة من الاحتيال المصرفي منها:
- اختلاس النقد والموارد المالية الأخرى.
- توزيع أو تحريف المستندات بما في ذلك طلبات التوظيف والقوائم والشهادات والمؤهلات أو مستندات الهوية أو بطاقات الصرف الآلي، أو البطاقات التجارية.
- توزيع التوثيق والوثائق.
- تزوير الأوراق النقدية.
- تغيير أحد أو كل أركان مكونات الشيك.
- سرقة بطاقات الصرف الآلي أو بطاقات الائتمان واستعمالها بطريقة غير شرعية.
- تخيل تعيينات وبيانات غير سليمة من خلال الحاسب الآلي.
- سوء استخدام المعلومات وسرويرها بطريق غير شرعي.
- تحويل أموال لعملاء ومهمين أو موظفين أو بأعما.
- خلق الرشاوى أو الهدايا أو العوائد السرية لمنح طلب أو تجاهل الإجراءات المتخذة وحالات عدم الالتزام أو كافعة تقدم مكافح بما في ذلك الوصول إلى معلومات سرية.
- الحصول على طريق الاحتيال على منافع أو مستندات لا يحق للمستلم أن يحصل عليها.

5-2 دور التقنية:

أتسببت التقنية الحديثة في قطاع المصرفي أنها سلاح ذو حدين. فمن ناحية اسلفت جهود مكافحة الاحتيال بشكل واضح من التقنية الحديثة إذ أن الاحتيال قد تمتلك على النظام الآلي، على سبيل المثال، قد خضع من آنات اختلاس النقود لحادثات حياة النقود، كما أن تطوير وسائل وأدوات لاستشغال الاحتيال يعد الفضيل فيه إلى أدوات التقنية المتطرفة.

ولكن من ناحية أخرى فقد برر المحتجون باستخدام أحدث التقنيات لتعزيز قدرتهم. ويمكن القول أن لا شيء قد سهل الاحتيال أكثر من الانتشار الواسع لأجهزة الحاسب الآلي زهيدة المين وعالية القدرة والموفرة بتصرف مما弥补لها من التقنيات أخرى. فتقنيات المستندات الحالية مثل مسح النطاقات البصرية وطبع النطاقات والمراجع المختلفة قد سمح بأعمال تزوير بصفة جد أكثراً. فوسائل تزوير الشباكات السببية في السابق قد حاولت فيها أعمال تزوير عالياً الجودة لدعم الأوراق المالية القابلة للتداول بما في ذلك الشباكات
by highly efficient methods, allowing forgery acts of all tradable securities, including checks, letters of credit, promissory notes and bonds. As the Saudi banks have made great progress over the preceding period in the introduction of electronic technology into their systems, it is likely that the number of acts of forging documents would decrease while the developed technological level of forgery and its monetary value will likely increase.

Modern technologies have also allowed forging of currencies and credit cards widely, an activity well-known to organized crime gangs. Forging major currencies, in particular, is being practiced at the international level in coordination with money-laundering gangs.

The modern technologies have led to further exposure to the risks of financial losses, apart from the old risk of fraud related to "Insider Trading" acts. When a bank's employee changes indebtedness position fraudulently or when a broker carries out unapproved deals or exceeds the limit of the deal, both acts will expose the bank to potential catastrophic losses in a short period of time.

Using internet for banking activity also exposes banks to new risks. Skillful fraudsters, who use latest technologies and deeply know the underlying deficiencies of internal control procedures at banks, represent an increasing danger of Cyber Crime.

It is not expected that the information about cyber crime mentioned in these guidelines would cope with the rapid advancement of technological development. Therefore, banks should always be acquainted with the latest technological methods used by fraudsters so as to be able to detect, control and combat fraud. For this purpose, the internal systems and procedures must continually be developed for observing and analyzing fraud trends to develop appropriate means to combat it. These important developments shall then be summarized and circulated to the bank's employees. The plan to combat and control fraud mentioned in these guidelines include a number of suggestions.

2-6 SAMA’s Circulars & Supporting Guidelines

SAMA has issued a number of circulars concerning fraud. To obtain these circulars, refer to "(SAMA’s Circular Manual) - Section 120 entitled "Economic Crimes". The following table describes briefly sub-sections of the circulars related to economic crimes in this Manual:

2-6 SAMA’s Circulars & Supporting Guidelines

SAMA has issued a number of circulars concerning fraud. To obtain these circulars, refer to "(SAMA’s Circular Manual) - Section 120 entitled "Economic Crimes". The following table describes briefly sub-sections of the circulars related to economic crimes in this Manual:
<table>
<thead>
<tr>
<th>Section</th>
<th>Circular Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>120/1</td>
<td>Notifying authorities concerned of fraud operations</td>
</tr>
<tr>
<td>120/2</td>
<td>Guidelines to combat financial embezzlement and fraud</td>
</tr>
<tr>
<td>120/3</td>
<td>Guidelines to combat money-laundering</td>
</tr>
<tr>
<td>120/4</td>
<td>Attempts of forging the national currency and efforts to combat them</td>
</tr>
<tr>
<td>120/5</td>
<td>Attempts of forging foreign currency and efforts to combat them</td>
</tr>
<tr>
<td>120/6</td>
<td>Attempts of forging documents and efforts to combat them</td>
</tr>
<tr>
<td>120/7</td>
<td>Other banking fraud operations</td>
</tr>
<tr>
<td>120/8</td>
<td>Committee for Resolution of Banking Disputes</td>
</tr>
<tr>
<td>120/9</td>
<td>Committee for Combating Embezzlement and Financial Fraud</td>
</tr>
<tr>
<td>120/10</td>
<td>Bank Treasury Committee</td>
</tr>
<tr>
<td>120/11</td>
<td>Banking complaints and disputes</td>
</tr>
<tr>
<td>120/12</td>
<td>Currency counting and examination machines</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>كلمات التوجيه</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1/120</td>
<td>إبلاغ السلطات الأمن بأعمال الاحتيال</td>
</tr>
<tr>
<td>2/120</td>
<td>إرشادات لمكافحة الابتزاز المالي والاحتيال</td>
</tr>
<tr>
<td>3/120</td>
<td>إرشادات لمكافحة غسل الأموال</td>
</tr>
<tr>
<td>4/120</td>
<td>محاولات تزييف العملة الوطنية وجهود مكافحتها</td>
</tr>
<tr>
<td>5/120</td>
<td>محاولات تزييف العملات الأجنبية وجهود مكافحتها</td>
</tr>
<tr>
<td>6/120</td>
<td>محاولات تزوير المستندات وجهود مكافحتها</td>
</tr>
<tr>
<td>7/120</td>
<td>أعمال احتيال بنكي آخر</td>
</tr>
<tr>
<td>8/120</td>
<td>لجنة تنسيق المنازعات المصرافية</td>
</tr>
<tr>
<td>9/120</td>
<td>لجنة مكافحة الاختلاس والاحتيال المالي</td>
</tr>
<tr>
<td>10/120</td>
<td>لجنة خزينة البنك</td>
</tr>
<tr>
<td>11/120</td>
<td>الدعاوى والمنازعات البنكية</td>
</tr>
<tr>
<td>12/120</td>
<td>عد العملات ومكائن للفحص</td>
</tr>
</tbody>
</table>
SAMA has also issued a number of guidelines and supporting booklets that should be read along with these controls. They include the following:

- Manual of Guidelines for Combating Embezzlement and Financial Fraud
- Managing operational risks through insurance programs.
- Internal control guidelines for commercial banks.
- Accountancy criteria for commercial banks.
- Minimum conditions for actual security.
- Minimum conditions for security systems.
- Rules governing the opening of bank accounts in Saudi Arabia and General operational Guidelines.
- Directions for security guards.
- Procedures of protecting cash money during transportation.
- Guidelines on combating and control of money-laundering activities via banking system.
- Guidelines on internet banking security.

3- Plan for Combating Fraud

3-1 Introduction

It is necessary for every bank to set an integrated plan to combat fraud so as to address all aspects of the fraud problem. These guidelines suggest 9 basic conditions to develop an effective plan to combat fraud in commercial banks by building on and adopting the best international practices in this area. These conditions are the following:

First: A strategy to combat and prevent fraud.
Second: Regulatory framework and responsibility structuring.
Third: Assessing fraud risks.
Fourth: Spreading awareness with regard to fraud.
Fifth: Control procedures.
Sixth: Control and follow-up.
Seventh: Fraud notification methods.
Eighth: Investigation criteria.
Ninth: Conduct and disciplinary criteria.

These conditions and guidelines are general, not detailed. They contain a list of issues that need to be addressed in depth by any bank in accordance with its own circumstances. The bank is responsible for developing the necessary measures, standards, systems and procedures for effective application and follow up of these conditions as part of an ongoing campaign launched by the bank with all its sections and departments to combat fraud.

The conviction of how important is risk management represents an essential part of combating fraud. By using management techniques, the management can clearly determine most...
deficiencies of controls and take proper measures to redress wrong control mechanisms or introduce additional techniques.

The following sections discuss the basic nine conditions separately. Each section starts with a general brief introduction, followed by specific guidelines aimed at helping banks in their efforts to address their own requirements.

3-2 The First Basic Condition: Strategy of Fraud Combat and Control Policy

3-2-1 Introduction
Each bank shall have a comprehensive and integrated written policy for fraud combat and control along with the supervision details on fraud and corruption combat. This policy shall draw all procedures and measures appropriate for the bank concerned, along with a wide range of complementary anti-fraud procedures. The policy must adopt the risk management method to combat and control fraud. The main purpose of the policy is to promote awareness and compliance among employees, determine the bank’s departments in charge of combating and controlling fraud, and applying the plan’s various aspects of combating and controlling fraud. To assess the effectiveness of the plan, it must be followed up and assessed internally and externally.

3-2-2 Guidelines
1. The bank must lay down and promulgate a written policy for fraud combat and control; and it should be circulated to its staff.
2. This policy must include the bank’s control measures for combating fraud and corruption, set the goals to be achieved, and should combine the existing policies and measures related to fraud and corruption combat.
3. The policy can be presented in one document or in a set of booklets, instructions, circulars, and guidelines which generally explain the elements of the bank’s strategy.
4. The policy must be based on the bank’s risk analysis in terms of its internal and external environment and it should adopt the method of risk management for fraud control (This aspect is included in the basic third condition entitled “Assessment of Fraud Risk”).
5. The policy must be comprehensive and cover the bank’s essential functions and activities.
6. The policy must be integrated without any conflict between independent elements.
7. As a minimum, the policy must cover the basic conditions stated in 3-1.
8. The policy of fraud combat must define in details
the members of the fraud combat committee, its business scope and purposes. The committee, which consists of senior officers from the bank’s various departments, shall be responsible for the development, application and coordination of the policy (refer to the second basic condition entitled “Regulatory Framework and Responsibility Structuring”).

9. Executive officials must set a good example of integrity regarding compliance with the essence and provisions of the policy of combating and controlling fraud. They must also realize that they are responsible and accountable for creating and preserving an ethical atmosphere that would help in thwarting fraud and encouraging notification of any violation of acceptable standards.

10. The bank must designate sufficient staff members and resources to ensure the success of the policy of combating and controlling fraud. Senior officials’ clear commitment in terms of the designated time and resources would help in sending a clear message to the employees that the management will not be lenient in combating corruption.

11. All employees must be aware of their responsibilities regarding the combat, detection, notification, and investigation of fraud (refer also to the fourth basic condition entitled “Promoting Awareness of Fraud”).

12. It will be appropriate that the operational organ participate in drafting the policy of fraud combat to determine potential areas where corruption may take place and how it can be minimized.

13. It is important to keep the operational organ always informed of the developments, application, accomplishments and benefits of the policy in order to promote compliance with the policy’s purposes on the broadest scale.

14. Joint action and promotion of regulatory culture help banks to benefit from accumulated expertise and ideas.

15. The policy of combating and preventing fraud must be adapted and updated in so far as to reflect developments in the bank and its operational environment. For this purpose, the policy and its efficiency to achieve the reappraised goals must be periodically reviewed, at least every two years; or whenever changes occur in the operational environment which may weaken the capacity of such policy to combat and control fraud, and its ability to meet reassessed objectives.
3-3 Second Basic Condition: Regulatory Framework and Responsibility Structuring

3-3-1 Introduction
A comprehensive and effective regulatory framework as well as a structure of responsibilities must be developed to execute the comprehensive policy of fraud control approved by the bank, partially by application of sound domestic control systems. A fraud control committee must be formed to lay down the policy, coordinate and follow up its application, and provide the necessary support to its chief executive. All levels of management must be involved in the implementation of this policy.

3-3-2 Guidelines
1. The regulatory responsibility for adopting the bank’s comprehensive fraud-combat strategy and each of its elements must be clearly determined and the bank’s management and employees must be informed thereof.

2. There must be an independent committee as mentioned in 3-3-1 concerned with fraud combat and control in the bank, and the following is recommended:
The task of a fraud control committee is to lay down, coordinate and follow up a policy for fraud detection and investigation.
Defining the responsibility for fraud control in clear terms.
Applying a clear structure to notify of fraud acts.

3. Roles and responsibilities of all employees must be documented clearly in the policy for combating and controlling fraud. Each employee must know whom to call and what he should do when suspecting a fraud act.

3-3-2-1 Management Responsibilities
1. The bank’s management is responsible for fraud combat. Therefore, it clearly bears the responsibility for laying down and determining the regulatory responsibility for fraud combat and prevention.

2. Studies issued by international administrative consultation firms indicate that the behavior of senior officials and executives is one of the most important aspects of creating an ethical atmosphere in any institution. Therefore, good behavior starts at the top of the pyramid and goes down to the base through the conduct of senior officials who must first behave with integrity and adopt the principles they advocate. In view that the conduct of an employee and its stand inside a big financial institution are affected greatly by the senior management, directors should set a good example by following valid control procedures in the

3-3-4 1 مسؤوليات الإدارة

1-الإدارة هي المسؤولة عن مكافحة الاحتيال. لذلك تتحمل الإدارة بشكل ثان مسؤولية وضع وتحديد المسؤولية التنظيمية لمكافحة الاحتيال.

2-تلزيم الدراسات الصادرة عن الشركات العالمية لل мастерات الإدارية أن سلوك كبار التنفيذيين في البنك هو من أهم جوانب خلق مناخ أخلاقى في أي منشأة. لذلك يجب أن يبدأ السلوك الصحيح من قمة الهرم و ينتقل تدريجيا إلى القاعدة عبر تصرف كبار المسؤولين بنزاهة وممارسة ما يدانوه به. و ينظر أن سلوك الموظف وما تواجهه داخل المنظمة المالية الكبرى تتاثر كثيراً بإدارة العليا. إذا تعين على المدير أن يكون القدوة بإتباع إجراءات الرقابة الصحية في أعمالهم اليومية و لعدم الأعمال الانتقائية بحكم مواقفهم.
performance of their daily work, and should not violate regular procedures as a result of their positions.

3. Studies also indicate that the more the board of directors understands in depth banking operations, the less the bank will be exposed to fraud acts. Since the employee’s behavior and actions in large institutions are greatly affected by the senior management, the executives must set a good example in following proper control measures in their daily work and should not violate regulatory rules and procedures because of their higher positions.

4. Executives must realize the allegiance responsibility associated with their position in detecting and combating fraud. The responsibilities of the management for detecting and combating fraud must be documented at a strategic level in the management’s plans and operation booklets.

5. At the operational level, the responsibility of management for detecting and combating fraud must be defined in the job descriptions, and in the head office and branches’ circulars and code of conduct.

6. Directors must provide the necessary guidance and support for employees regarding notification of suspected fraud. If employees notified of dishonest practices and did not receive necessary support from the management, credibility of the policy of fraud control would be undermined.

7. The official to be responsible for fraud cases should enjoy broad responsibilities in the bank. This task should not necessarily be a separate job. One of the bank's employees may be entrusted with this task in addition to his job provided that conflict among responsibilities must be avoided. But it is necessary that the person assigned for this mission be given sufficient authority to deal with fraud effectively. In some cases, the official in charge of fraud cases must have the right of direct access to the top chief executive.

3-3-2-2 Fraud Control Committee

A fraud control committee plays a major role in setting a policy to combat fraud; and should ensure that policies, measures and procedures included in the comprehensive strategy for fraud control are applied effectively. The committee oversees the development of the elements contained in the nine basic conditions for combating and controlling fraud mentioned therein.

A fraud control committee must be formed to lay down the policy, coordinate and follow up its implementation, and to provide support to the top chief executive, provided that the mission of fraud combat and control shall not be confined to this committee. Rather, all levels of management and employees must be properly involved in promoting, coordinating, and continually following up fraud

3-3-2-2 لجنة مراقبة الاحتيال:

تعتبر لجنة مراقبة الاحتيال لدى البنك دوراً رئيسياً في وضع السياسة والتنفيذ من السياسات والإجراءات والتدابير التي تتضمنها الإستراتيجية العامة لمراقبة الاحتيال. يُشجع تطبيقها بصورة فعالة.

وتشير إلى تطوير عناصر الشروط الأساسية للتعامل مع الكفالة المالية الاحتيالية والاحتيال الوراثة في هذا الدوام.

إنشاء لجنة لمكافحة الاحتيال لوضع السياسة وتسهيل ومتابعة تنفيذها.

وتشجع حالات الاحتيال التي تسبب، على أنها تكون موضوعًا لجنة مراقبة الاحتيال الوراثية. يجب أن تتعاون جميع مسؤوليات الإدارة والموظفين بالطرق الصحيحة في تسهيل سياسة مكافحة الاحتيال والاحتيال الوراثي. تحدد سياسة مكافحة الاحتيال لدى البنك أعضاء اللجنة ومسؤولياتها.
The bank’s fraud combat policy must determine the committee’s members and responsibilities. The committee must include senior officials, representing major business areas at the bank. The committee must meet regularly, monthly if possible, or at least once every three months. There must be a possibility to hold emergency meetings to discuss serious suspected cases of fraud. One of the committee’s main tasks is to notify of fraud and give support to the top chief executive regarding all aspects of the bank’s fraud-combat policy.

3.3.2.3 Fraud Investigation Unit
The fraud investigation unit’s role shall be to investigate potential fraud cases against the bank. This responsibility shall include collecting and presenting the necessary evidence to support administrative, disciplinary, or other measures such as prosecution and recovery of the funds subject of the fraud operation. In addition to conducting the investigation role, the investigation unit must provide the following:

- Support, information, and advice to the fraud control committee.
- Support the detection and combat of fraud and promote awareness thereof.
- Support and guidance for the training on fraud combat.
- Reports to SAMA’s fraud database on a periodical basis as instructed by SAMA.
- Periodical reports on fraudulent cases shall be submitted to the executive management.
- Technical reports on recommendations to overcome deficiencies in the internal control systems and policies and procedures manuals.
- Notifying insurance companies and submitting claims to them for compensating incurred losses of fraud.

A fraud database must be established for use by the fraud combat unit. Therefore, this unit could be the best group at the bank to maintain such a database. The executive management may decide to assign the responsibility of this task to another unit at the bank. The database is an important instrument for detecting and combating fraud and managing the bank’s policy of fraud control. For easy reference and determination of accountability, the database must contain all details about actual and suspected fraud cases.

The fraud database must keep, as a minimum, the following details about each fraud case:

- Reference number (relevant to related tangible records).
- The status quo (Has the file been closed or is it still active).
- Relevant information and dates, or the period in which the fraud occurred.

The fraud database must keep track of all fraud cases in the bank, including the status of each case and any related documentation. The database must be regularly reviewed and updated to ensure its accuracy and effectiveness.

3.3.2.3.1 Fraud Investigation Unit
The fraud investigation unit’s role shall be to investigate potential fraud cases against the bank. This responsibility shall include collecting and presenting the necessary evidence to support administrative, disciplinary, or other measures such as prosecution and recovery of the funds subject of the fraud operation. In addition to conducting the investigation role, the investigation unit must provide the following:

- Support, information, and advice to the fraud control committee.
- Support the detection and combat of fraud and promote awareness thereof.
- Support and guidance for the training on fraud combat.
- Reports to SAMA’s fraud database on a periodical basis as instructed by SAMA.
- Periodical reports on fraudulent cases shall be submitted to the executive management.
- Technical reports on recommendations to overcome deficiencies in the internal control systems and policies and procedures manuals.
- Notifying insurance companies and submitting claims to them for compensating incurred losses of fraud.

A fraud database must be established for use by the fraud combat unit. Therefore, this unit could be the best group at the bank to maintain such a database. The executive management may decide to assign the responsibility of this task to another unit at the bank. The database is an important instrument for detecting and combating fraud and managing the bank’s policy of fraud control. For easy reference and determination of accountability, the database must contain all details about actual and suspected fraud cases.

The fraud database must keep, as a minimum, the following details about each fraud case:

- Reference number (relevant to related tangible records).
- The status quo (Has the file been closed or is it still active).
- Relevant information and dates, or the period in which the fraud occurred.

The fraud database must keep track of all fraud cases in the bank, including the status of each case and any related documentation. The database must be regularly reviewed and updated to ensure its accuracy and effectiveness.
which the fraud was committed.
The name or names of fraudsters and relevant persons, whether among the bank’s employees or persons from outside the bank.
Estimation of the fraud’s resulting material value and the entire impact on the bank’s transactions or performance.
The geographic or physical location of the fraud.
The nature or the focal point of the fraud.
Indicating the methods used in the fraud (the practices which took place).
The procedures taken concerning the investigation conducted.
The investigation results.
The disciplinary action, for example, compensation and/or the prosecution that took place.
The measures taken to combat fraud.
The fraud investigation unit must be in charge of training and qualifying investigators.

3.3.2.4 Combating and Detection
It should be ensured that an effective system is in place for controlling fraud, which should firmly control the risks of fraud by detecting, tracking and controlling fraudulent acts to take prompt actions to reduce the potential fraud losses and maintain confidentiality.

Setting up measures to ensure continuous prosecution of or to enforce disciplinary measures on the employees involved in dishonest business.
Enhancing and strengthening the existing policies and controls as required.
Establishing a central unit to which all fraud cases alleged of employees or the public will be referred.
Reviewing the process of hiring and selecting employees, screening and testing them regarding fraud risks.
Ensuring the implementation of effective measures on employees.
Determining the process of recovering any incurred losses, such as settlement of claims, reduction of losses and damages, the recovery process and insurance claims management.
Informing the management of the cases of conflict of interests, violations of the bank good policies and customers’ complaints.
Determining the sequence of reporting and making decisions on suspected fraud cases.
Giving advice and required modifications for internal control to combat fraudulent activity.
Setting policies for protecting those who cooperate to detect fraud.
Reviewing the results of fraud risks assessment.
Ensuring that all fraud control initiatives are given priority and implemented continuously.
Setting systems for reporting to SAMA.
Giving assistance in arbitration and settling disputes which the fraud was committed.

The name or names of fraudsters and relevant persons, whether among the bank’s employees or persons from outside the bank.
Estimation of the fraud’s resulting material value and the entire impact on the bank’s transactions or performance.
The geographic or physical location of the fraud.
The nature or the focal point of the fraud.
Indicating the methods used in the fraud (the practices which took place).
The procedures taken concerning the investigation conducted.
The investigation results.
The disciplinary action, for example, compensation and/or the prosecution that took place.
The measures taken to combat fraud.
The fraud investigation unit must be in charge of training and qualifying investigators.

3-3-2-4 Combating and Detection
It should be ensured that an effective system is in place for controlling fraud, which should firmly control the risks of fraud by detecting, tracking and controlling fraudulent acts to take prompt actions to reduce the potential fraud losses and maintain confidentiality.

Setting up measures to ensure continuous prosecution of or to enforce disciplinary measures on the employees involved in dishonest business.
Enhancing and strengthening the existing policies and controls as required.
Establishing a central unit to which all fraud cases alleged of employees or the public will be referred.
Reviewing the process of hiring and selecting employees, screening and testing them regarding fraud risks.
Ensuring the implementation of effective measures on employees.
Determining the process of recovering any incurred losses, such as settlement of claims, reduction of losses and damages, the recovery process and insurance claims management.
Informing the management of the cases of conflict of interests, violations of the bank good policies and customers’ complaints.
Determining the sequence of reporting and making decisions on suspected fraud cases.
Giving advice and required modifications for internal control to combat fraudulent activity.
Setting policies for protecting those who cooperate to detect fraud.
Reviewing the results of fraud risks assessment.
Ensuring that all fraud control initiatives are given priority and implemented continuously.
Setting systems for reporting to SAMA.
Giving assistance in arbitration and settling disputes
among internal groups regarding honesty and operation of loss provisions.
Continuously reviewing effectiveness of the comprehensive strategy and various elements of each of the nine basic conditions.

Fraud Analysis:
Establishing a protected and unified database for all fraud cases.
Reviewing the status quo of all fraud cases notified.
Reviewing the fraud cases notified.
Determining the details and weaknesses of internal controls, procedures and operations.
Analyzing trends, determining reasons and assessing incidents regularly.

Awareness:
Determining the needs and proper training programs for educating employees about fraud.
Supervising education and awareness programs on fraud.
Briefing continuously of the developments and issues of fraud control in general and disseminating the information of the best practices on fraud through bulletins and other means of communications circulated among all divisions of the bank.

Investigation into Fraud:
Determining the policy of how to address fraud and give advice and assistance to the units engaged in the investigation.
Conducting initial assessments of all proven fraud cases.
Approving disciplinary measures (This can be done in other ways).

Notification
Ensuring timely and continuous notification of all fraud cases. This includes all information on domestic and foreign branches, internal and external incidents, and actual and potential or suspected fraud.
Submitting statistical reports to the management.
Submitting reports and the minutes of sessions of the committee to the Risk Management Review Group.
Submitting reports to the Accounts Auditing Committee on fraud cases and implementing the strategies included in the plan of Fraud Control.

3-3-2-5 Employees’ Responsibilities
In compliance with the bank’s fraud-control policy, employees must undertake the following:

3-3-2-5 مسؤوليات الموظفين:
تبدأ سياسة مراقبة الاحتياط لدى البنك، بتعين على الموظفين القيام
Familiarize themselves with the concepts and responsibilities of fraud control. The staff should sign in acknowledgement of their knowledge.
Take sound financial, legal and ethical decisions during their daily duties and responsibilities.
Accept the responsibility of fraud control in their field of work.

### 3-4 Third Basic Condition: Assessment of Fraud Risk

#### 3-4-1 Introduction

Fraud is part of the operational risk. To ensure whether the management has the necessary information to address fraud, a periodical structural review must be conducted to assess fraud risk, including all functions and operations of the bank. This review must address both internal and external fraud risks, and determine the level and nature of the bank’s exposure to fraud risks. Thus, the management can decide the anti-fraud measures it deems necessary. All new products and services must undergo this assessment operation to determine whether the fraud risk has been minimized. It is only this official risk assessment process which can determine and assess fraud risks and indicate what measures have been taken and the measures that need to be taken to minimize such risks.

#### 3-4-2 Guidelines

The assessment of fraud risk must be reviewed periodically and it should include all functions and operational units in the bank, provided that this review should address both internal and external fraud risks to determine the level and nature of the bank’s exposure to such risks. The analysis of fraud risk will enable the development of a plan for fraud control compatible with the risks indicated.

At first, all new products and services must undergo risk assessment process to ensure whether such risks have been minimized and manageable.

To ensure the preservation of the current state of the bank’s exposure to fraud risk, a periodical review of risk assessment must be conducted every two or three years (or at a shorter period if important structural changes have taken place in the bank.)

This periodical review provides an opportunity to reassess all risks specified in the previous assessment. It also provides a chance to include the risks previously identified in the risk assessment of new products introduced by the bank.

In accordance with international trends, to make the board of directors more responsible for the operations of the bank under their management, the

3-4-3 الشرط الأساسي الثالث: تقييم مخاطر الاحتيال :

- Familiarize themselves with the concepts and responsibilities of fraud control.
- Take sound financial, legal and ethical decisions during their daily duties and responsibilities.
- Accept the responsibility of fraud control in their field of work.

Familiarize themselves with the concepts and responsibilities of fraud control. The staff should sign in acknowledgement of their knowledge.
Take sound financial, legal and ethical decisions during their daily duties and responsibilities.
Accept the responsibility of fraud control in their field of work.

3-4-3-1 مقدمة : 

بما يلي:

- الإعلان والتعريف بمفاهيمهم ومسؤوليات مراقبة الاحتيال ، مع أخذ توقيعهم بالعلم .
- اتخاذ قرارات مالية وتنظيمية وأخلاقية سليمة أثناء قيامهم بمهامهم ومسؤولياتهم المصرفية.

- قبول تحمل المسؤولية عن مراقبة الاحتيال في مجال عملهم ومسؤولياتهم .

3-4-3-2 العوامل: 

- تشترك محصلة جزء من الخطر التشغيلي . وفي سبيل المثال من أن الإدارة تمتلك المعلومات اللازمة في معالجتها لمعالجة الاحتيال، يجب إجراء مراجعة هيكيلية دورية لتقييم خطر الاحتيال الشامل شامل ووضائف وعمليات البنك وتعالج هذه المراجعة أخطار الاحتيال الداخلي والخارجي على حد سواء وأد تطبيق إحساس البنك لمخاطر الاحتيال. عندما تستطيع الإدارة أن تقرر التدابير الحضادية التي تدعو الحاجة إليها . تختص جميع المنشآت والخدمات الجديدة

- عملية تقييم هذه إضافة إلى مراجعة المخاطر كفارة لذلة السياسات والإجراءات المتعلقة بذلك المنشآت والخدمات لمعرفة إذا ما قد تم تخفيف خطر الاحتيال، وتحديد تلك العملية قادرة على تحديد تقييم مخاطر الاحتيال وتبادل ما هو التدابير التي اتخذت و양ظات ما زالت هناك حاجة لاتخاذها لتقليل وتحقيق هذه المخاطر.

3-4-3-3 الإرشادات: 

- إجراء مراجعة تقييم مخاطر الاحتيال دوريًا بحيث تشمل جميع الوظائف ودفات التنفقات في البنك على أن تتم هذه المراجعة مخاطر الاحتيال الداخلي والخارجي على الوسائط لتحديد مستوى طبيعة تعرض البنك لهذه المخاطر. ويمكن تحليل مخاطر الاحتيال بتطوير خطة احتيال الإدارية وتوزي المخاطر الحضادية. قبل بدء تخصيص جميع المنشآت والخدمات المالية الجديدة لعملية تقييم المخاطر ويشمل ذلك معرفة ما إذا كان قد تم تخفيف هذه المخاطر وإمكانية إدارتها.

- تتضمن مناحي الاحتيال بالضرورة لمواجهة الخطر الاحتيال، من الملاحظ إجراء مراجعة دورية لتقييم المخاطر كل ستين أو ثلاثة

- أو أقل من ذلك إذا واجه البنك تغييرات هامة في حيويته.

- توفر هذه المراجعة الدورية فرصة لإعادة تقييم جميع المخاطر المحددة في الفحوص السابق إضافة إلى توفير الفرصة لدمج المخاطر التي تبقى تحديدًا من المراجعة السابقة أثناء تقييم المخاطر للمناطق الجديدة

- التي أدخلتها البنك على عمله.

- تتشوار مع الاتجاهات العالمية لجعل أعضاء مجلس الإدارة أكثر

- مسؤولية عن أعمال البنك، لتحمل الإدارة المسؤولية عن إجراء تقييم مسؤولية عن أعمال البنوك
bank’s management shall bear the responsibility for conducting an assessment of fraud risk. The internal and external auditors are expected to participate significantly in that assessment, or make sure that the assessment process has actually taken place. The assessment process must be considered an important administrative tool, rather than a process limited to account auditor’s scope of work.

3-4-2-1 Assessment Process of Fraud Risk
The fraud risk assessment process usually goes through several stages, as follows:

Determining the major jobs at the bank.
Assessment and classification of the general nature of each work field and to what extent it is susceptible to fraud.
Identifying the specific forms of fraud risk in each field.
Assessment of the possible occurrence of specific risks in light of the counter factors, such as internal controls.
Assessment of the potential impact on the bank as a result of the occurrence of specific risks.

Suggestion and development of strategies to minimize or eliminate specific risks entirely.

The suggested strategies, in the final stage of risk assessment process mentioned above, may lead to taking specific anti-fraud measures; making additions and amendments to operational measures or the existing controls; or introducing new regulations and controls.

To minimize risks, a certain person, committee or a specific group inside the bank must be held responsible for each strategy.

There must be a detailed timetable for each item requiring a certain measure. The fraud control committee at the bank is to provide the appropriate mechanism to follow up the application of the specified measures.

The process of fraud risk assessment must be recorded and documented properly for future reference and accountability purposes.

3-5 Fourth Basic Condition: Promoting Awareness of Fraud and Making Employees understand that Fraud is not permissible:

3-5-1 Introduction
The management must realize that the employee’s participation in fraud combat is essential, and that most fraud cases will not be detected or controlled without the employees’ cooperation. In order to increase the awareness of the employees and emphasize the bank’s commitment to combat fraud, the need arises for a series of continuous initiatives to raise the issues of fraud combat, detection and notification thereof before all employees. The
training for fraud combat and control must be an obligatory element of the employees' training. There may be a need for updating appropriate documents, such as booklets on the best practices.

As for the public, there is also a need to inform customers and raise their awareness of the fact that fraud against the bank is forbidden, and fraudsters will be referred to competent authorities.

3-5-2 Guidelines
The management should realize that employees participation in combating fraud is an essential matter and that most fraud acts cannot be detected or prevented without employees' co-operation.

3-5-2-1 Employee's Awareness
To draw the attention of all employees to the issue of combating, controlling and notifying of fraud, a cohesive awareness program should be established. Training seminars on promoting awareness of fraud and security may need a combination of elements and implications so as to be effective. The starting point for training shall become a message requiring each employee to bear the responsibility of participation in the combat and control of fraud.

Discussion seminars and training materials should use, as far as possible, relevant realistic examples of real cases happened in the bank's history or in other banks.

Promoting awareness and discussion seminars can be used to support official training seminars on control and security systems. Discussion topics may include certain issues, such as the bank's policy for controlling fraud (Overview), ethical and cultural issues, the management and employees' responsibilities, and code of conduct and notification of fraud.

Educational visual aids can be used in seminars, curricula, shows and discussion groups. It is worth mentioning that previously prepared visual aids are cheaper than those made by the bank. However, some banks may find it difficult to obtain previously prepared visual aids.

Guidance booklets on the best practices could serve as guidelines and references. Other printed communication materials, which can be used to reinforce the message of combating fraudulence time after time, using different methods, could include news letters, fact statements, posters and notes. To be informed of the methods and means of advertising and promoting public awareness of how to combat fraud, reference can be made to the warning and awareness strategy undertaken by SAMA in co-operation with commercial banks.

Systems should be developed to follow up and evaluate sources of information about the best
practices, and to distribute relevant information. The internet can also be used to pass on information inside the bank rapidly and extensively. There is a need for special training to address the demands of participants in selected seminars. Exploitation of corruption opportunities, corruption and illegal benefits, which are often connected with such seminars, may be reduced if participants are trained to define and avoid misconduct and conflict of interests. All participants should provide statement denying any interest (see the Fifth Basic Condition entitled “Internal Control Procedures” for information on the guidelines for avoiding conflict of interests).

The code of Conduct at a bank would serve as guidelines on moral expectations and responsibilities inside the bank. Therefore, the code of conduct represents the starting point of the campaign for the promotion of ethical conduct at work and its main element (In this connection, see the Ninth Basic Condition entitled “Conduct and Disciplinary Standards”).

3-5-2-2 Promotion of Customer's Awareness
There is a need to raise public awareness of the fact that fraud committed against banks and their customers is forbidden, and that fraudsters will certainly be referred to competent authorities. The public should be informed that it is responsible, on its part, towards the banks; and banks, on their part, are responsible and accountable for funds held in their custody. Thus, the public, for example, has the right to presume that banks should take all appropriate and reasonable measures to control fraud.

An alert customer plays an important role in helping detect and combat external fraud. To this end, he should support and provide information on fraudulence acts by promptly notifying of such crimes. Annual reports and news letters would help the customer to be always informed of the status quo. Periodical information and advertising campaigns can also be used to inform the public of the types of fraud against banks and the ways of detecting them.

3-5-2-3 Promoting Awareness of Concerned Parties
Banks should always understand the importance of concerned parties with whom contracts are made that code of conduct, the banks’ policy of combating and controlling fraud and other banks' policies and standards regarding fraud and corruption are instruments used to promote justice, integrity and accountability. Contracts must provide for adherence to ethical values and integrity. As part of the evaluation subsequent to contracting, results in terms of quality and integrity should be evaluated.
The Fifth Basic Condition: Internal Control Procedures

Introduction

Internal controls are the main instrument for combating fraud. Therefore, sound internal control regulations should be set within a framework of a written documented comprehensive policy and rules of procedure to lessen opportunities for committing fraud acts. The strategy for combating and controlling fraud should also be integrated with the inclusion of operational procedures and rules governing the activities of all departments, cash handling facilities, jobs and employees.

Controls are measures used to minimize risks at work to the lowest level. They are designed to prevent, detect and redress mistakes in due course through applying the instructions related to the following:
- Employees
- Leaves
- Substitution of alternatives
- Job rotation
- Training
- Approvals and authorizations.

Evidences. Settlements.
Review of operational performance.
Security of assets.
Separation of duties.

Controls can be classified as follows:
Preventive controls: to prevent the occurrence of unfavorable incidents (such as front-end access controls, including passwords, combinations, proofs, evidence, limits and actual barriers).
Detection controls: to detect and remedy unfavorable incidents which have already occurred (i.e. back-end controls), such as proofs, evidence, reviews, settlements and results of audited accounts and reports.
Guidance controls: to urge and encourage doing favorable actions (such as policies, procedures, code of conduct and guidance booklets).

Internal controls include basic precautionary measures, such as separation of duties. Employees in charge of actual safeguarding of assets must not also be responsible for accountability for these assets and verification of audit statements. Technologies of effective control enable the bank to:

Discover mistakes upon their occurrence, and thus avoid heavy losses.
Protect employees with integrity against illegal manipulation by other employees or the bank’s customers.

Collect all evidence necessary to identify dishonest employees and customers, prosecute and arrest them.

SAMA requires all banks to put into effect internal control systems as stated in details in "the Directory of Internal Control Guidelines for Commercial Banks". These are comprehensive range of guidelines governing all activities of commercial banks in the Kingdom. To generally understand SAMA’s requirements regarding commercial banks’ internal control systems, “Internal Control Guidelines” shall be read together with the section on “Control Guidelines for Combating Fraud”, as well as other relevant circulars and work instructions. Adoption of these guidelines, procedures and work instructions is the most important element of a bank’s comprehensive strategy to create a well fortified environment against fraud.

The above-mentioned guidelines do not represent a comprehensive list that covers all areas governed by "Commercial Banks' Internal Control Systems". However, they aim at:

- Emphasizing the importance of internal controls in combating and controlling fraud.
- Highlighting some main principles of effective internal control.
- Providing additional information and guidelines with the aim of reinforcing "Internal Control Guidelines".

**3-6-2 Guidelines**

Sound internal control regulations within a framework of a comprehensive written documented policy and clear comprehensive rules of procedure should be put into effect to lessen the opportunities for fraud acts.

The strategy of comprehensive internal control should be closely integrated into the operational documents governing all departments, cash handling facilities, jobs and employees.

Banks shall examine the "Manual of Internal Control Guidelines for Commercial Banks" to find out examples of internal control guidelines, methods and procedures. In additions, Banks should be guided by SAMA’s guidelines and circulars, as well as all laws in force that govern banking activities in the Kingdom to fully understand in detail the formal provisions for internal controls.

The following guidelines aim at emphasizing the information on internal control procedures set forth in the documents referred to above.

3-6-2-3 The above-mentioned guidelines do not represent a comprehensive list that covers all areas governed by “Commercial Banks’ Internal Control Systems”. However, they aim at:

- Emphasizing the importance of internal controls in combating and controlling fraud.
- Highlighting some main principles of effective internal control.
- Providing additional information and guidelines with the aim of reinforcing “Internal Control Guidelines”.

**Guidelines**

Sound internal control regulations within a framework of a comprehensive written documented policy and clear comprehensive rules of procedure should be put into effect to lessen the opportunities for fraud acts.

The strategy of comprehensive internal control should be closely integrated into the operational documents governing all departments, cash handling facilities, jobs and employees.

Banks shall examine the "Manual of Internal Control Guidelines for Commercial Banks" to find out examples of internal control guidelines, methods and procedures. In additions, Banks should be guided by SAMA’s guidelines and circulars, as well as all laws in force that govern banking activities in the Kingdom to fully understand in detail the formal provisions for internal controls.

The following guidelines aim at emphasizing the information on internal control procedures set forth in the documents referred to above.

**Guidelines**

Sound internal control regulations within a framework of a comprehensive written documented policy and clear comprehensive rules of procedure should be put into effect to lessen the opportunities for fraud acts.

The strategy of comprehensive internal control should be closely integrated into the operational documents governing all departments, cash handling facilities, jobs and employees.

Banks shall examine the "Manual of Internal Control Guidelines for Commercial Banks" to find out examples of internal control guidelines, methods and procedures. In additions, Banks should be guided by SAMA’s guidelines and circulars, as well as all laws in force that govern banking activities in the Kingdom to fully understand in detail the formal provisions for internal controls.

The following guidelines aim at emphasizing the information on internal control procedures set forth in the documents referred to above.
3-6-2-1 Main Principles of Effective Internal Control
Written effective internal controls shall govern the following:
Restricted and monitored access to risky areas.
Actual maintenance and safeguarding of valuable assets, including facilities, assets, registers and intellectual property.
Proper authorization and definition of levels of approval for all employees.
Efficient separation of duties, especially in financial and accounting areas, and delivery and taking-over of cash or securities.
Record of all transactions, incidents, suspected transactions and findings of investigation.
Extraordinary or unexpected findings of investigation.
Notification methods.
Accountability for results at all levels.
After their application, control regulations shall always be followed up and regularly reviewed to test their effectiveness. The collapse of the oldest commercial bank in the U.K., "Bearings Bank" in 1995, is an example of ineffective control. The official investigation proved that the bank's collapse was due to unauthorized catastrophic activities practiced at the wrong time by a seemingly one person who was undiscovered because management and internal controls, which are basic factors of banking, were weak and deficient.

The overall justification for not abiding by the controls was that such controls were no longer logical, there was no sufficient time or they were invalid. It is important to inform the management of these comments to see if there is a need for assessment of such controls.
During periods of significant regulatory changes, the risk of weak accountability for parts of the work and vagueness about notification responsibilities would increase. Under such circumstances, the senior management must clearly emphasize areas of responsibility and separate follow up of the internal controls at each stage of transformation.

3-6-2-2 Practices of Personnel
Statistics show that the greatest risk of fraud faced by a bank is usually posed by its employees, either in or without cooperation with outsiders.
It should be remembered that employees at their various post levels can currently commit a large portion of the assets of the bank and assets of its customers through their business activities. This entails giving more attention to the integrity of all employees.
An employee's integrity should be considered a precondition for the success of any control system.
Test of integrity before contracting with an employee should be strictly made so as to have reliable and trustworthy employees. Managers, apart from depending on the information on the detailed employment application form and other references, should be trained in the skills of interrogation to ensure that they can determine the occurrence of dishonorable act in the employee's history and expect that such act could likely happen in the future. The bank should record the references named by the nominated employee and compare them with other separate references. Educational and professional qualifications should also be verified.

Before contracting with a new employee, it is important to ensure that he has not already been involved in fraud or embezzlement acts in a financial firm inside or outside the Kingdom, by reviewing information presented by the applicant, and making sure of its validity and contacting his references; and undertaking necessary procedures to prevent appointment of employees of past fraudulent conduct.

Prior to concluding contracts with new employees, it should be ensured that an employee is not working in another job and intends to continue therein. It should also ensured that he is not engaged in a commercial activity in order to achieve the principle of protection against conflict of interests. This shall also apply to the staff of companies having contracts therewith.

It is necessary to continually follow up an honest behavior. An extensive number of indicators "red lines" are now available to help managers in identifying individuals who are likely to commit fraudulent acts. These red lines usually include behavioral and social characteristics as follows:

- Unjustified enrichment and sudden change in the style of living.
- Loss of original documents and substituting them with their copies.
- Overuse of correction fluids.
- Hesitation about leave-taking.
- Refusal of promotion.
- Rapid resignation of a new employee.
- Insistence of some suppliers, contractors or customers on dealing with a certain employee.
- Intimate relationship with suppliers, contractors or customers which breaks suddenly.

Control must also be performed over old employees who have acquired a broad knowledge about security procedures at the bank, particularly if disputes arise regarding work, or if the bank is overstaffed.

Employees should be provided with clear written documents for informing them about important matters, such as job description, policies, procedures
and instructions of work that explain all aspects of their duties and responsibilities.

An employee shall be aware of all his rights and responsibilities regarding all issues related to fraud. Follow-up and control methods should include the following:

Confidentiality agreements.

Obligatory leaves.

Change of an employee's duties schedules and tasks at unexpected intervals.

Checking the accounts of an employee who is on leave.

Employees who are relatives should not be allowed to work together, particularly in financial, accounting, cash handling or securities areas.

Photos of an employee must be taken to be available to the bank in case he disappeared or was blackmailed.

A bank should fully consider the implications of earlier employees' actions of not giving explicit references, and those who are proven to have committed such acts must be dismissed from their jobs.

### 3-6-2-3 Separation of Duties

The principle of separating tasks and duties should be strictly applied to all operational areas and activities where applicable. This principle basically requires that jobs entailing performance of operational tasks must be separated from those entailing the enforcement of controls and supervision. Similarly, control of assets must be separated from control of documents related to these assets.

The following examples are collected from different areas of work to clarify the principle of duty separation:

1. The tasks of receiving and release of guarantees in favor of borrowers must be separated from the task of registering the guarantees.
2. The task of debt collection must be separated from the task of fixing the amount of debt.
3. The task of payroll must be separated from the other tasks of personnel affairs.
4. Trading transactions at the front offices must be separated from those at the back offices. Although traders are required, for instance, to observe limits, they must be strictly controlled by the back or the middle office.
5. The tasks of ordering purchase of consumable materials and equipment, and storage control must be separated from the task of keeping records and authorization to pay. The Manual of "Internal Control Guidelines for Commercial Banks" includes several cases in which effective separation of duties is required.

### بالاحتفال.

تشمل الأسباب المتصلة بالرقابة ما يلي:

- اتفاقيات الصرف.
- الإجازات الإلزامية.

تدبِر برامج الموظف ومهم عمله على قدرات غير متوقعة.

تتفق حسابات الموظف الذي يذهب في إجازة.

لا يجوز أن يصبح الموظف من ذوي القدرات أن يعمل مباشرةً، لا سيما في المجالات المالية والملاحية وتسليم وصابرة النقد أو الأوراق المالية.

ومر على أخذ مجموعة من الصور المقطوعة للموظف للمساعدة في حال اختفاء أو في حال كان ضحية لمحاولة ابتزاز.

يرجى أن يولي البنك كل اهتمام لبعض الموظفين السابقين عن إعطاء مراجع صريحة. يجب صرف المرتكبين الثانيين من الخدمة دون مرجع ومتطلباتهم.

### 3-6-2-3  فصل الوظائف:

تطبيق مبدأ فصل الوظائف والواجبات بكل سرية في جميع المجالات والأنشطة التشغيلية حيث يطبق ذلك. يتطلب هذا المبدأ أساسًا فصل الذين يودون واجبات تشغيلية عن أولئك الذين يغتنم الصوابع ويتوكلون مهمة الرقابة. كذلك الأمر فصل الرقابة على الموجودات عن رقابة المستندات المتعلقة بهذه الموجودات.

فعلى سبيل المثال، وسائل العلل المتصلة بفصل ملاحظة العمل بناءً مبدأ فصل الوظائف.

1. فصل وظائف استلام الضمانات والإدراج عنها إلى المفترضين عن توقيعات في تسجيل ضمانات.
2. فصل تحصيل الدين عن وظيفة تحديد.
3. فصل مهمة حمل الرواتب عن مهم إدارة الموظفين.
4. فصل عملية التحقيق في المكتب الأساسي والمكتب الخفي، مع أن المطلوب من المطلوبين، مثلاً، أن يبررون اختمار التحقيق، لا يد
5. فصل وظائف تبليد شراء المواد الأولية لاستهلاك المعدات ونود التخزين عن وظيفة استلام السجلات والاحتفاظ بها وتعذر التفتيح.

وتضمن "إرشادات الرقابة الداخلية للبنوك التجارية" إشارة عدة لحالات تطلب فصل الوظائف بشكل خاص.

and instructions of work that explain all aspects of their duties and responsibilities.

An employee shall be aware of all his rights and responsibilities regarding all issues related to fraud. Follow-up and control methods should include the following:

Confidentiality agreements.

Obligatory leaves.

Change of an employee's duties schedules and tasks at unexpected intervals.

Checking the accounts of an employee who is on leave.

Employees who are relatives should not be allowed to work together, particularly in financial, accounting, cash handling or securities areas.

Photos of an employee must be taken to be available to the bank in case he disappeared or was blackmailed.

A bank should fully consider the implications of earlier employees' actions of not giving explicit references, and those who are proven to have committed such acts must be dismissed from their jobs.

### 3-6-2-3 Separation of Duties

The principle of separating tasks and duties should be strictly applied to all operational areas and activities where applicable. This principle basically requires that jobs entailing performance of operational tasks must be separated from those entailing the enforcement of controls and supervision. Similarly, control of assets must be separated from control of documents related to these assets.

The following examples are collected from different areas of work to clarify the principle of duty separation:

1. The tasks of receiving and release of guarantees in favor of borrowers must be separated from the task of registering the guarantees.
2. The task of debt collection must be separated from the task of fixing the amount of debt.
3. The task of payroll must be separated from the other tasks of personnel affairs.
4. Trading transactions at the front offices must be separated from those at the back offices. Although traders are required, for instance, to observe limits, they must be strictly controlled by the back or the middle office.
5. The tasks of ordering purchase of consumable materials and equipment, and storage control must be separated from the task of keeping records and authorization to pay. The Manual of "Internal Control Guidelines for Commercial Banks" includes several cases in which effective separation of duties is required.

### بالاحتفال.

تشمل الأسباب المتصلة بالرقابة ما يلي:

- اتفاقيات الصرف.
- الإجازات الإلزامية.

تدبِر برامج الموظف ومهم عمله على قدرات غير متوقعة.

تتفق حسابات الموظف الذي يذهب في إجازة.

لا يجوز أن يصبح الموظف من ذوي القدرات أن يعمل مباشرةً، لا سيما في المجالات المالية والملاحية وتسليم وصابرة النقد أو الأوراق المالية.

ومر على أخذ مجموعة من الصور المقطوعة للموظف للمساعدة في حال اختفاء أو في حال كان ضحية لمحاولة ابتزاز.

يرجى أن يولي البنك كل اهتمام لبعض الموظفين السابقين عن إعطاء مراجع صريحة. يجب صرف المرتكبين الثانيين من الخدمة دون مرجع ومتطلباتهم.

### 3-6-2-3  فصل الوظائف:

تطبيق مبدأ فصل الوظائف والواجبات بكل سرية في جميع المجالات والأنشطة التشغيلية حيث يطبق ذلك. يتطلب هذا المبدأ أساسًا فصل الذين يودون واجبات تشغيلية عن أولئك الذين يغتنم الصوابع ويتوكلون مهمة الرقابة. كذلك الأمر فصل الرقابة على الموجودات عن رقابة المستندات المتعلقة بهذه الموجودات.

فعلى سبيل المثال، وسائل العلل المتصلة بفصل ملاحظة العمل بناءً مبدأ فصل الوظائف.

1. فصل وظائف استلام الضمانات والإدراج عنها إلى المفترضين عن توقيعات في تسجيل ضمانات.
2. فصل تحصيل الدين عن وظيفة تحديد.
3. فصل مهمة حمل الرواتب عن مهم إدارة الموظفين.
4. فصل عملية التحقيق في المكتب الأساسي والمكتب الخفي، مع أن المطلوب من المطلوبين، مثلاً، أن يبررون اختمار التحقيق، لا يد
5. فصل وظائف تبليد شراء المواد الأولية لاستهلاك المعدات ونود التخزين عن وظيفة استلام السجلات والاحتفاظ بها وتعذر التفتيح.

وتضمن "إرشادات الرقابة الداخلية للبنوك التجارية" إشارة عدة لحالات تطلب فصل الوظائف بشكل خاص.
3.6.2.4 Dual Control

As security measures (such as the use of keys, warning systems and security of cash locations) must be subject to strict dual control technologies, the following instructions shall be taken into consideration:

To lessen the opportunities for getting duplicate keys without authorization, employees may not, by all means, share keys belonging to dual guard. This shall also be applied to combinations of the vault under dual watch.

Key boxes should not contain a bunch of "emergency keys" in the form of unauthorized duplicate keys under dual control.

Lost key must be notified of at once, even if duplicate keys are available.

If an employee suspects that the confidentiality of one of the combination numbers placed under dual watch has been cracked, he must report the incident immediately.

There must be a procedure to recover keys and other methods of entry on a periodical basis. Measures must be made on a periodical basis to ensure the replacement of keys, passwords and other instruments of dual watch.

The control officer must always attend while checking designated cash locations and ATMs.

Since fraudsters often use the period that immediately follows the checking process to perpetrate embezzlement, two full-checking processes must be made to the cash handling facilities when detecting a considerable error in the calculation of balance on hand. The first checking process shall be made upon detecting the error and the second shall be made after identifying the cause of the error.

3.6.2.5 The Policy of Gifts

Since an employee is prone to bribery by the gifts given to him to distract his attention from suspected transactions, a written policy must be set for preventing this and how to include this provision in the bank’s policy for combating fraud, and in the employee’s booklet prepared by the bank.

This policy shall generally prohibit the employee from the following:

Accepting any gifts, enticement or inappropriate entertainment for providing lawful or unlawful service.

Revealing confidential or restricted official information for any enticement.

Abusing his previous and current jobs to get differential prices for private transactions.

3.6.2.5 The Policy of Gifts

Since an employee is prone to bribery by the gifts given to him to distract his attention from suspected transactions, a written policy must be set for preventing this and how to include this provision in the bank’s policy for combating fraud, and in the employee’s booklet prepared by the bank.

This policy shall generally prohibit the employee from the following:

Accepting any gifts, enticement or inappropriate entertainment for providing lawful or unlawful service.

Revealing confidential or restricted official information for any enticement.

Abusing his previous and current jobs to get differential prices for private transactions.
3.6.2.6 Dormant Accounts
The control of dormant accounts shall be a continuous policy. See “the Guidelines of Internal Control” and SAMA’s relevant circulars to learn about the instructions for dormant accounts.

3.6.2.7 Cash Handling (Delivery and taking-over)
There is a number of risk exposure cases in the area of cash handling which are governed by a set of procedures (see “the Guidelines of Internal Control” in this regard). These procedures must be implemented properly by making surprise visits for regular checking of balance on hand in vaults and teller’s departments. Exposure to cash risks includes activities that are related to the following:
Control and management of cash in the bank’s till.
Transfer of cash from vault to the bank’s till.
Access to the tellers’ till and cash when the teller is off work or away from the till, even for a short time.
The actual status and the security of locks and vaults.

To ensure proper accountability for cash, the cash handling procedure to tellers at the bank’s branches, and to other employees working in the field of cash handling must be clear and consistent. The guidelines related to the seals of the teller and other instruments of marking, authorization forms, keys, passwords and the set of combination numbers must be implemented, followed up and evaluated regularly to ensure their ongoing effectiveness.

Places designated for tellers shall be closed, and persons authorized to enter those areas shall be specified.

3.6.2.8 Limits of withdrawals
The limits of overdraft, its amount and transactions shall be determined where applicable to tellers, traders, officials and other employees dealing in cash and in non-cash financial instruments or negotiable documents. These limits shall reflect the potential risks and the level of risk that can be borne by the management. These limits shall be followed up accurately and implemented strictly.

3.6.2.9 Supervision of the Trading Room
Clear separation of duties in the trading room or rooms at a bank is an essential requirement for any effective control system. The term “back office” usually includes the records of the activity of trading, settlements and adjustments. Often, and on necessity, the “back office” employees work closely with those engaged in selling and purchasing operations on a daily basis.
However, development of this close relation at work must not be permitted to prevent traders from controlling the “back office”. The activities of trading shall be supervised by a separate team entrusted with the task of risk management as a part of continuous management of all sorts of risks. The task of this team is to conduct independent inspection to ensure that traders are trading within their designated limits and that any trading beyond these limits must be reported and authorization is obtained immediately, and that sensitivity towards market fluctuations and their impact on the financial position have been evaluated and reported. This inspection team shall ensure that profits and losses are recalculated regularly, and registered in the accounting records, and if necessary, in the records kept by the traders.

Banks shall have documented measures and controls covering all aspects of transactions progress, its calculations and notification thereof. Employees who are asked to deviate from these measures and controls must ask about the reason, and if they are not convinced of the answer, they should be encouraged to report the case to the senior management.

The internal auditor shall audit the activities of the trading room strictly and regularly. The management shall cautiously look into the cases in which a single individual seems to be able to answer all the main questions about a certain activity or product. It is necessary to establish clear reporting lines and effective communications among senior officials, especially when overseas or geographically remote branches are involved in trading operations.

Where banks have international transactions, the integrity of controls related to the business of overseas offices should not be infringed. The managers in charge must conduct frequent visits at reasonable intervals to overseas branches carrying out trading business, especially when the branch is distant from the head office. These visits shall include discussion of trading activities with traders, risk managers, branch managers and supporting employees, in addition to talks with the competitors of the branch’s activities and its traders. The management can not be sure of receiving the correct information, asking the right questions and its power to interpret warning signs correctly unless it has a proper understanding of the work and how it is conducted.

The domestic management of the overseas branches may not be involved in taking daily decisions of such branches; however, it must have the power to ensure adherence of these branches to the control standards set by the bank (e.g. by making surprise inspections).
There is a great risk of not including extraordinary activities (like some complex derivative transactions) in the work structure of banks; and thus they may be poorly managed and controlled. Therefore, these activities must be governed by a high level of administrative control. The main principle of prudent management is to maintain strict rules regarding verification and correction in the tasks of settlements irrespective of whether the payments will go to the group’s companies or to a third party.

3.6.2.10 Conflict of Interests Management
Banks shall set and implement policies and measures to prevent and solve conflict of interests. These measures shall be documented in the employee’s booklet and other relevant instruction directories. The code of conduct must include or refer to the policy concerning conflict of interests. Customers, external institutions, contractors, job applicants and bank employees themselves have the right to expect the bank to perform its obligations in a fair and unbiased manner; and the bank’s policy must not be influenced by self interest or personal gain. Conflict of interests arises when the bank’s employees fall or seem to have fallen under the influence of personal interests during their work. Perceptual recognition of conflict of interests might be harmful as much as actual conflict because it undermines confidence in the integrity of the bank concerned and its employees. Conflict of interests may involve a financial gain that might occur when, for example, a bank’s employee or a member of his family owns a real estate or shares or occupies a position in a company which bids for a contract with the bank, and at the same time he receives gifts, entertainment or income from another job. It is not necessary that there is a pecuniary price because conflict of interests may emerge by choosing a certain bidder to win a contract, or appointing one of the relatives or friends in a certain position. Areas of potential conflict of interests shall be determined as part of assessing the risk of fraud. Areas of work at the bank where conflict of interest can occur include the following: Bids and purchases. Appointment of employees. Work without payment and part-time jobs (trainees). Gifts, benefits and entertainment. Approving loans and other forms of credit. Dealing in securities. The bank’s senior officials, any director, or any other employee working as a member of a
recruitment committee or a bids selection committee, or a member of any other internal team that engages in selecting, approving, setting a policy or making a decision shall disclose to the bank in writing if they have any interests concerning their work which might affect their ability to participate in the evaluation tasks neutrally. A typical interests’ register shall be used for this purpose.

Interests that must be considered as “relevant and important”, are the following:

1. Ownership of shares in firms which may seek to deal with the bank.
2. Ownership of shares in firms which may prepare the specifications, their commercial relations with the suppliers participating in the bid.
3. Full or partial ownership of shares in private companies (excluding inactive companies).

Additional measures should be put into effect to reduce the possibility of dishonest activity between employees participating in the decision making process and suppliers by setting certain rules of procedure requiring potential suppliers to disclose any commercial, intimate, social or kinship relation with any bank’s employee or with the potential suppliers.

The procedures of assessing the bids of competing suppliers must be assessed.

The procedure of selection and approval may begin at the beginning of the meeting, and this disclosure shall be recorded in the minutes of the session. If conflict of interests emerges during the meeting, the member concerned shall withdraw from the meeting and not participate in the discussion or relevant decision.

The procedure of selection and approval may possibly lead to the emergence of a conflict of interests which results in giving preference to a certain competitor over another one in awarding the contracts. To reduce this probability, the following steps shall be taken:

1. The specifications of the required services must not be prepared in a way that gives preference to a certain supplier. When consultants are needed to prepare the specifications, their commercial relations with the suppliers participating in the bid must be assessed.
2. The procedures of assessing the bids of competing providers may not be prepared in a way that gives preference to a certain provider. This shall implicitly indicate that the participants in selecting bidders must disclose any financial interest or social relation or kinship with the potential suppliers.
3. Measures should be put into effect to reduce dishonest activity between employees participating in the decision making process and suppliers by setting certain rules of procedure requiring potential suppliers to disclose any commercial, intimate, social or kinship relation with any bank’s employee or with the potential suppliers.

The procedure of selection and approval may possibly lead to the emergence of a conflict of interests which results in giving preference to a certain supplier over another one in awarding the contracts. To reduce this probability, the following steps shall be taken:

1. The specifications of the required services must not be prepared in a way that gives preference to a certain supplier. When consultants are needed to prepare the specifications, their commercial relations with the suppliers participating in the bid must be assessed.
2. The procedures of assessing the bids of competing providers may not be prepared in a way that gives preference to a certain provider. This shall implicitly indicate that the participants in selecting bidders must disclose any financial interest or social relation or kinship with the potential suppliers.
3. Measures should be put into effect to reduce dishonest activity between employees participating in the decision making process and suppliers by setting certain rules of procedure requiring potential suppliers to disclose any commercial, intimate, social or kinship relation with any bank’s employee or with the potential suppliers.
participating in choosing one of the competitors.
4. While traders work as managers of relations with customers when undertaking the responsibility of trading for the bank’s own account, potential risks such as inadequate allocation of transactions and concealing deals of personal accounts are inevitable. To reduce these risks, the management must impose accurate and strict controls.

3.6.2.11 Protection of Intellectual Property
The bank’s definition of “material security” shall include the protection of the bank and its customers’ data in addition to other intellectual properties such as systems and computer programs (applications and software) that are internally developed by the bank. The places in which these data are stored shall be protected against any internal or external risks, and only those who need such data shall be permitted to have access to them. In addition, access to those data shall be controlled by entry systems via keys, cards and secret numbers.

Every employee or firms working for the bank or on its behalf shall fill in and sign a regular undertaking to maintain confidentiality. The undertaking shall specify in detail the responsibilities for improper disclosure of this information. Confidential information is defined as the information owned by the bank and not available to the public, and only a related individual or the bank itself can have access to it.

For security reasons, data and contingency policies stored on back-up discs and other hardware media must be stored in remote locations.

Waste papers shall be shredded or disposed of; other media such as data discs shall be destroyed safely.

A clear office policy shall be followed to maintain confidentiality. This policy shall be designed in a way ensuring that employees transfer all confidential and restrictively distributed or sensitive information when they are off work for a long period of time, especially at the end of each working day. These items shall be removed from the employee’s office and locked up in a safe storage area designated for each employee and each office.

The bank shall regularly review and update the measures and policies of internal control in order to deal with new risks related to embezzlement or illegal access to privately-owned information.

3.6.2.12 Information Systems Security
Detecting the activity of “Cyber Terrorists” is a crucial element in protecting the information network and its systems. However, most hackers’ acts into bank networks are committed inside the bank itself by insiders, such as current employees, unauthorized employees and other related parties participating in choosing one of the competitors.

'Cyber Terrorists' is a term used to describe hackers who use cyber attacks to disrupt the operations of financial institutions. These hackers can be employees, former employees, or outsiders who have gained unauthorized access to the bank's systems.

- 2021-03-01

- 2021-03-01

- 2021-03-01
who know how to do harm to the bank specifically, severely and swiftly. The policy of combating and controlling fraud shall include a methodology or code of conduct for using computers. This security policy shall determine the standards of using computer hardware and software at the bank, and it shall include instructions about using the bank’s internet, e-mail and permission to have access to the internet. Network administrators shall be in the lead in assessing weaknesses of the network, determining the best sites for implementing security measures and highlighting forbidden activities. Proper instruments shall be used for security management to ensure the integrity, confidentiality and accessibility to the network. "Integrity" means, in this context, that the information is accurate and protected against accidental or deliberate modification. "Confidentiality" means that the information is only accessible to those who are authorized to know it. Technological administrative instruments enable managers to centrally manage the user’s adherence to security policies, implementing such policies, detection of valid security breaches and tracking them, check the system to determine its vulnerability to be hacked into, issue comprehensive reports on normal usage of the network, and thwart the attempts of certain privileged employees to misuse the network. All changes in processing systems need approval, documentation and follow up.

3.6.2.13 Fraudulent Invitations

A bank might find itself invited to play a role in a deal fraudulent in its essence. Such invitation is usually introduced as a complicated deal of a high financial value, offering attractive opportunities for low-cost finance or high-return investment. These invitations usually involve financial instruments (e.g. certificates of deposit, bonds or preferred banking collateral) that carry the name of an unknown or geographically isolated financial institution. A good example in this regard is what is done by a number of international fraudulent unions, known as "Advance Free Fraud/Tele fax Scam". These invitations represent direct financial risks that defame the bank’s reputation. The ultimate purpose of fraudsters may be to get a payment (e.g. pre-paid fee). However, their goal of getting close to the bank might be to have documents that add credibility and respect to their fraudulent methods. Even a letter that does not include a business offer might provide access to the core of the bank’s documents or to get a signature of one of the members of its board of directors.

If the bank is offered any important deal by a person, not an old and trustworthy customer or a director of an international company, the bank shall be instructed not to receive any documents from the person and to not contact him for the deal. Such invitations represent direct financial risks that defame the bank’s reputation. The ultimate purpose of fraudsters may be to get access to the core of the bank’s documents or to get a payment (e.g. pre-paid fee). However, their goal of getting close to the bank might be to have documents that add credibility and respect to their fraudulent methods. Even a letter that does not include a business offer might provide access to the core of the bank’s documents or to get a signature of one of the members of its board of directors.

The bank might offer any important deal by a person, not an old and trustworthy customer or a known or geographically isolated financial institution. A good example in this regard is what is done by a number of international fraudulent unions, known as "Advance Free Fraud/Tele fax Scam". These invitations represent direct financial risks that defame the bank’s reputation. The ultimate purpose of fraudsters may be to get a payment (e.g. pre-paid fee). However, their goal of getting close to the bank might be to have documents that add credibility and respect to their fraudulent methods. Even a letter that does not include a business offer might provide access to the core of the bank’s documents or to get a signature of one of the members of its board of directors.
financial partner, it must take a very cautious approach by verifying the deal’s nature, sources and the person recommending it.

The following is a list of descriptions that may serve as indicators to warn the bank against the nature of a fraudulent deal:

Country of origin – A bank should be careful and cautious depending on the country of origin.

Confirming the intent of partnership – the perpetrators of the deal often request a written confirmation of intent from the bank at an early stage of its desire and capacity to engage in the deal. Any documents sent in response to their request of this sort will be used for committing fraud.

Ratio of unrealistic returns – To attract investors, borrowers and other shareholders to the deal, the perpetrators of the fraudulent act offer high, unrealistic returns and low cost of borrowing as an incentive for participation. In addition, it is probable that the deal’s value is high.

• Confidentiality and penalty conditions:
  The invitation requires that the nature of the deal and/or its parties remain confidential for competitive reasons. It may not be disclosed except after all parties sign the agreement or after the payment of specified fees. The confidentiality conditions may include fines in the case of non-commitment.

• Complexity:
  The deal is often very complex, without any apparent reason in some cases. It is likely that the fraudsters overuse an incomprehensible language to give the impression of having profound knowledge.

• Use of fax and the internet:
  Most of the documents, if not all, exchanged between the parties, are sent via fax or the internet, facilitating counterfeiting of letters and concealing the place of residence of intermediaries and fraudsters.

• Fees of third parties:
  Because the project involves funds, payments are often required for third parties who clearly have nothing to do with the project.

3-7 Sixth Basic Condition: Follow-up Process

3-7-1 Introduction

The management should ensure that an independent and reliable follow-up process is in place. Internal follow-up and control activities should be enhanced by regular support from independent external evaluators, such as external auditors.

3-7-2 Guidelines

The management should ensure that an independent and reliable follow-up process is in place.

The ongoing internal follow-up and control activities are usually the function of the internal auditors, the risk management, quality safety
management or internal control.
It is necessary to support the internal follow-up by an independent, regular assessment conducted by external evaluators, such as external auditors. The management must act quickly after receiving the reports of external auditors to fix deficiencies of the control, follow-up and ensure its implementation.
The fraud control committee shall follow-up the effectiveness of the policy to control and prevent fraud.

3-7-2-1 Internal Follow-up
Following up the internal controls shall begin as the board of directors, managers and supervisors begin performing their daily activities in the areas of supervision, inspection, control and guidance or by employing control procedure and Control of Risk Self Assessment (CRSA).
The board of directors may rely on experts in the management to conduct the daily works of the bank, but it remains solely responsible for the follow-up of the bank's activities. It can follow-up the bank's activities through administrative reports, but it shall do more than receiving and reviewing these reports. It shall ensure that such reports are accurate and reliable. Therefore, the internal administrative reports prepared by the bank must be sound enough insofar as to allow the management to rely upon them for making decisions and follow up their impact afterwards.
Members of the board and senior managers must be fully satisfied that the bank's risk management and internal control systems are operating properly. The executive management bears the basic responsibility for achieving such satisfaction. The board of directors may decide to seek a neutral opinion independent from that of the executive management. Internal account auditing is an important source in this regard within the bank, because it undertakes the task of the application of an ongoing control program.
Internal account auditing reviews the operating procedures issued by the board and ensures that they are subject to adequate controls, working properly and adhering to the board's policies, and laws and regulations in force.
Internal auditing represents a point of continuous focus on internal controls and periodical control of all the aspects of the bank's work. The internal auditor should review the adherence of the bank to approved policies and regulations and laws in force. Although the bank is responsible for deciding on the number of times required by the internal auditor to review specific transactions, the areas in need of more auditing include those vulnerable to the greatest potential risk (such as the risk of fraud in this case), or those which have shown a weakness in the previous reviews.
The more the size of business, its risk, its complexity, or its geographical expansion, the more is the need for experienced, professional and skillful internal auditors.

The internal auditor must coordinate his activities with external auditors and provide them with basic information. The head of internal auditing must enjoy absolute power to have access to the senior executive, and the chairman of the board of directors and the head of the auditing committee regardless of the person to whom the reports are submitted.

One of the responsibilities of the bank’s auditing committee shall be to ensure the effectiveness of internal audit tasks.

When preparing internal audit reports, main points of weakness in the control must be highlighted. Afterwards, an administrative plan of action and a timetable shall be agreed upon to address the weaknesses. The management shall be responsible for implementing the recommendations of internal audit and making sure to properly address deficiencies on their appearance. If deficiencies emerge again, the internal auditor must plan to make subsequent visits within a short period after auditing to ensure that corrective measures have been taken.

If the management failed to implement the recommendations of the internal auditor, the account auditing committee should be informed.

It should be noted that the internal auditors cannot automatically prevent fraud. They principally work as supervisors responsible for ensuring that accounting standards are being applied, the administrative procedures are implemented properly, and the bank complies with local regulations and laws. Therefore, the task of developing the work plans and operational procedures to deal with potential fraud must be entrusted to the risk management, operational audit units or similar units.

A number of institutions consider this task as part of the overall risk management mission, supported and assisted by the internal audit and other departments concerned with the development of strategies for addressing problems related particularly to fraud.

It is proposed that a bank create an independent function for risk management to manage risks of all business activities and cover all aspects of risk. The main purposes of this function are to identify, analyze, assess and follow up the risks associated with any task or transaction within the bank to ensure that the activities of the bank are conducted pursuant to the policies of the board of directors regarding market risk, operational and credit risk. In this regard, risk management contributes significantly to the development of maintenance and following up internal controls.

Regarding the measures for controlling and combating fraud, specific tasks should be designated for internal auditing, risk management and quality assurance departments.
3-7-2-2 المتابعة الخارجية:

1. تقع على عاتق البنك المسؤولية تنفيذ قواعد ضوابط البنك الداخلية وتنويه مكتبات تدفقات الخدمات الداخلية والخارجية في البنك تنفيذ هذه المسؤولية. كما تقوم مؤسسة النقد تقييم أنظمة الضوابط الداخلية لدى البنك كجزء من برنامج خصيص من قبل المؤسسة. الفتيز على الشيخ خرجج هو أمر أساسي لتحقيق مستوى من أساليب التدقيق والضوابط الداخلية والضوابط التشريعي في البنك. وضوابط المعايير التشريعي من خلال البنك وضوابط المعايير الخارجية. كما يلزم المدفقات الخارجية فيما يتعلق بعنوان وإستراتيجية مهمة تدفق التدفق الداخلية لدى البنك ومجلس الإدارة يجب أن يكون على علم حول أداء مدفقات الخدمات الداخلية.

2. عدم المبالغة بفعالية التدقيق الداخلي في اكتشاف الانتهاكات ومحاسبته. لمراعاة الحسابات الخارجية يركز على تقييم التقارير المالية والأنظمة الداخلية لتوثيق مدى التقيد بالمعايير الداخلية والأنظمة الداخلية المثبتة. وقد يتم خطر الانتهاك عبر التقدير في مثل هذا النقد، فإن عمل المدفقات الخارجية يوفر مستوى معيين من ضبط الانتهاكات. ولكن الانتهاكات التي ادت إلى مدفقات الخارجيين استخدامها في التقدير لا تتضمن مصادر إضافية في مخاطر الانتهاك المتعلقة بالأعمال المرتبطة. كذلك يجب ملاحقة الانتهاك بصورة رئيسية عن طريق تدفق التدفق الداخلي والخارجي عنصرًا أخر من عناصر التدفق.

يمكن أن يؤدي استخدام المدفقات الخارجية كاستراتيجية للإدارة إلى

3. المسؤوليات العامة لرقابة البنك، ويرجع برنامج الرقابة عادةً سلسلة واسعة من الضوابط مثل حدود الأرقام المالية والضوابط وقضايا الأوراق المالية وشروط تدفق التقارير والكشف. وقد يتضمن من مسؤول (المدقق المالي) الانتهاك الإلزامي. أن.DecimalField المدقق المالي تendir أن أثر الضوابط والأنظمة الجديدة بالنسبة للانتهاك على أعمال إجراءات البنك وأن يتم الفحص بهذه الأنظمة والتعليمات وتدقيق مؤسسة النقد.

لا تعامل لمراقبة الانتهاك عادةً مباشرةً مع متابعة الرقابة الداخلية.

ويتوقف عملها في هذا الشأن على مجموعة الروك دالة حول جهود المتابعة التي يبذلها البنك لأعراف الإبلاغ المستمر عن سلامة ومكافحة الانتهاك.
which is another element of auditing.

The use of external auditors as advisors to the management may lead to a conflict of interests when, for example, they undertake the responsibility of setting an accounting system and are, requested later on to evaluate the system when performing external auditing. Therefore, banks and auditors shall strike a balance between potential conflict of interests and the cost of using one external auditor for interrelated work and the time to be saved. The prevailing professional standards allow an external auditor to perform a job not included in external auditing for one client, provided that the auditor's objectivity and independence must not be affected. The banks that wish to engage external auditors for other advisory services shall try to separate the advice the auditor can give from the administrative responsibility or operational execution, which may not be undertaken by an auditor.

3-7-2-3 The Policy of Following up Control and Combat of Fraud

The fraud control committee must follow up the implementation of the policy of combating and controlling fraud. The results of this follow-up must be reported to the senior management and the board of directors.

The following performance measures represent examples of major statistical indicators (in addition to any other measures prescribed by any particular bank), which can be used to follow up the effectiveness of a bank's measures to control fraud:

1. Extent of the difference between the risks assessed by the bank and risks assessed by insurance bodies.
2. The difference between the effectiveness of controls evaluated by the bank and those evaluated by insurance bodies.
3. Number of cases of normal suspected fraud and the number of such cases that have not arisen during the assessment of fraud.
4. Number of big suspected fraud cases and the number of such cases that have not arisen during the assessment of fraud.
5. Number of working days from the beginning of addressing fraud cases to the time when the addressing has ended.

The difference in the number of proven incidents of fraud and the amount of consequential lost funds and the number of alleged fraud cases referred to investigation and their value.

Number of times of recovery of funds and the amount of recovered funds in comparison to the number and value of alleged fraud cases referred to investigation.

The fraud control committee shall provide the executive management with regular reports on statistical operations listed above and update this information at least on a quarterly basis.

3-7-2-2 مراقبة الإحالة والتكميل:

توتلى جهاز مراقبة الإحالة متابعة تنفيذ سياسة مراقبة وكيفية الأخلاقية، و إبلاغ نتائج هذه المتابعة إلى الإدارة العليا و مجلس الإدارة.

تشكل الإجراءات التالية مسألة على المؤشرات الإحصائية الرئيسية (الحاصلة إلى أية إجراءات أخرى جدًا أي بنك معين) التي يمكن استنتاجها لMoslemi and ضمان الإحسانية. للمؤسسة ل сосуществة الإحالة. المراقبة. أسمى الإخلاص بين المشاطن في البنك، والذي تقييمه بناء على ضمان الهيأة.

3-7-2-3 The Policy of Following up Control and Combat of Fraud

The fraud control committee must follow up the implementation of the policy of combating and controlling fraud. The results of this follow-up must be reported to the senior management and the board of directors.

The following performance measures represent examples of major statistical indicators (in addition to any other measures prescribed by any particular bank), which can be used to follow up the effectiveness of a bank's measures to control fraud:

1. Extent of the difference between the risks assessed by the bank and risks assessed by insurance bodies.
2. The difference between the effectiveness of controls evaluated by the bank and those evaluated by insurance bodies.
3. Number of cases of normal suspected fraud and the number of such cases that have not arisen during the assessment of fraud.
4. Number of big suspected fraud cases and the number of such cases that have not arisen during the assessment of fraud.
5. Number of working days from the beginning of addressing fraud cases to the time when the addressing has ended.

The difference in the number of proven incidents of fraud and the amount of consequential lost funds and the number of alleged fraud cases referred to investigation and their value.

Number of times of recovery of funds and the amount of recovered funds in comparison to the number and value of alleged fraud cases referred to investigation.

The fraud control committee shall provide the executive management with regular reports on statistical operations listed above and update this information at least on a quarterly basis.
The internal auditing shall review the sound implementation of control and combating fraud policy at least biannually or after any significant changes in the areas of the bank business. The results of this review must be used to redevelop control and combating fraud policy to improve performance and enhance policies and procedures. This review must be followed by reassessment of the risk of fraud in the bank. This would not be possible unless all the units of the bank participate in the process of risk assessment and control of the risk on an ongoing basis, especially when significant changes occur in the business areas, job risks or controls.

3-8 Seventh Basic Condition: System of Notification of Fraud

3-8-1 Introduction
An official system shall be put into effect for internal notification of actual or suspected fraud. All staff must be clearly informed of the structure of the system and procedures for dealing with the notification of fraudulent acts. As part of this system, proper policies and mechanisms for the protection of suspects (if no proof was established of involvement in fraudulent acts) as a result of notification of fraudulent acts must be in place. Mechanisms should be developed to facilitate and encourage customers or the public in general to notify of cases of suspected fraud internally and externally. An official policy must be applied to external notification of certain authorities to SAMA and competent security authorities.

3-8-2 Guidelines
A system of internal notification of actual or suspected fraud must be put into effect. All staff must be clearly informed of the structure of this system and procedures for dealing with the notification of fraudulent act. Arrangements required will be affected by the size and structure of the bank (such as the number of branches, their locations and the number of operational units).
Initial training should cover structures and procedures of notification described in the employee's booklet and in the policy on combat and control of fraud.
An accurate concentrated summary on the arrangements of notification of fraud should be prepared for distribution to all staff and should be published regularly on bulletin boards and in internal newsletters.
To ensure proper conduct of reporters in following up their complaint, staff must be trained on the following:
How should they act if misconduct is seen at the work site.
What are the available internal notification mechanisms and how they work.
What are the preventive measures to protect those using notification mechanisms.
What are the available external notification channels.

Staff should be encouraged to file complaints without forgetting to mention their names. To this end, it is important that an employee should really be convinced that the complaint will be treated confidentially and that there are mechanisms in place to protect him against any reprisals.

An employee should be aware that any suspected fraud must be reported. The failed fraud act is as dangerous as a successful one that leads to a real loss of funds. If this unsuccessful attempt is not notified, the perpetrator will have an opportunity to try again with his fraudulent act.

Complainants must be informed that their complaints are taken into consideration and that appropriate measures will be taken. Complainants must be informed of the final results of all notified cases.

A motivation program shall be set up for employees who report cases of fraud once discovered.

3-8-2-1 Channels for Notification
Employees' complaints and notification reports must be submitted, in general, to their immediate superior. It is advisable that a written summary of the complaint be provided. The superior, on his part, shall submit it directly to the concerned member of the senior management.

If the notification is about the superior or if the employee has any valid fear of submitting the report to his immediate superior, there must be an alternative channel to submit a confidential report directly to the concerned member of the senior management.

If the notification report is against a member of the senior management, there must be a notification channel to the chief executive officer at the bank.

It would be advisable to have a telephone hot line which an employee can use for notifying of actual and suspected fraud acts. The hot line should be integrated with other notification channels and procedures mentioned in this section.

It is expected from the staff, in general, to follow the reporting channels within the bank. Nevertheless, employees must be informed that they may notify of any corrupt conduct directly to SAMA, if the employee is not willing to notify of it directly to his immediate superiors, to the concerned member of the senior management, or to the chief executive officer.

3-8-2-2 Protection of Notification
As a part of the system for notifying of fraud, proper mechanisms and policies must be developed for

What are the available internal notification mechanisms and how they work.
What are the preventive measures to protect those using notification mechanisms.
What are the available external notification channels.

Staff should be encouraged to file complaints without forgetting to mention their names. To this end, it is important that an employee should really be convinced that the complaint will be treated confidentially and that there are mechanisms in place to protect him against any reprisals.

An employee should be aware that any suspected fraud must be reported. The failed fraud act is as dangerous as a successful one that leads to a real loss of funds. If this unsuccessful attempt is not notified, the perpetrator will have an opportunity to try again with his fraudulent act.

Complainants must be informed that their complaints are taken into consideration and that appropriate measures will be taken. Complainants must be informed of the final results of all notified cases.

A motivation program shall be set up for employees who report cases of fraud once discovered.

3-8-2-1 Channels for Notification
Employees' complaints and notification reports must be submitted, in general, to their immediate superior. It is advisable that a written summary of the complaint be provided. The superior, on his part, shall submit it directly to the concerned member of the senior management.

If the notification is about the superior or if the employee has any valid fear of submitting the report to his immediate superior, there must be an alternative channel to submit a confidential report directly to the concerned member of the senior management.

If the notification report is against a member of the senior management, there must be a notification channel to the chief executive officer at the bank.

It would be advisable to have a telephone hot line which an employee can use for notifying of actual and suspected fraud acts. The hot line should be integrated with other notification channels and procedures mentioned in this section.

It is expected from the staff, in general, to follow the reporting channels within the bank. Nevertheless, employees must be informed that they may notify of any corrupt conduct directly to SAMA, if the employee is not willing to notify of it directly to his immediate superiors, to the concerned member of the senior management, or to the chief executive officer.

3-8-2-2 Protection of Notification
As a part of the system for notifying of fraud, proper mechanisms and policies must be developed for
supporting reporters and protecting them against reprisals as a result of their notification of fraudulent activities.

The employee's booklet and the bank's notification policy for controlling and combating fraud must indicate that severe penalties, including indictment of misconduct, legal prosecution and dismissal from work, shall be enforced against the person who harms any person notifying of fraud or a corruption act.

A person notifying of fraud shall not be protected if the investigation reveals that the notification has been reported due to malice or ill will.

Specific measures must be taken to eliminate the fear of retaliation and the prevailing feeling among employees that the one who notifies of fraud and corruption acts may get harmed. This message must be delivered to employees clearly and regularly through newsletters and other means of internal communication.

3-8-2-3 External Notification

Each bank needs to set a clear official policy and detailed procedures for notification of fraudulent acts and corruption to SAMA and concerned security authorities.

Fraud is a criminal act. When the bank believes after investigation that a proven act of fraud has been committed, the case must be referred to the police and reported to SAMA. Other firms, such as insurance companies, may also be concerned in certain cases and these should be identified as part of the bank's comprehensive policy.

Requiring the bank to notify of fraud shall not lessen its power to decide the appropriate treatment to be applied, such as legal prosecution, administrative measures, civil treatment or recovering money through disciplinary actions or refraining from taking any other measure.

Police intervention, especially when the amount involved is large, plays a significant role in alleviating the loss and damage resulting from fraud. The police may be able to intercept or freeze stolen money or to prevent the spoil of evidence through using its own resources or in cooperation with Interpol or any other international authority operating in the area of law enforcement. Therefore, it is important that the policy to combat fraud at the bank should allow taking a quick decision at the level of the executive management to implement actions, reduce the damage and protect the interests of the bank without any delay in cases of dangerous fraud and corruption.

The bank should inform SAMA of all serious fraud and suspected fraud cases. Notification of SAMA by a bank does not lessen its responsibility to refer fraud cases to the police or
other competent security authorities such as the Financial Investigations Unit (FIU), if necessary.

3-8-2-4 Receiving Notification Reports from Customers and the Public
Mechanisms must be developed to facilitate and encourage customers and the public in general to notify of suspected fraud cases, and external fraud. Banks, for example, shall consider the best method of how to receive complaints and reports on fraud from customers and ordinary citizens to deal with these complaints and reports. To this end, banks can make use of their web sites.

3-9 The eighth basic condition: Investigation Standards
3-9-1 Introduction
Staff at operation departments and those responsible for internal investigation must be provided with clear formal guidelines and procedures to ensure the treatment and investigation of fraud efficiently once detected. The roles and duties of the investigation organ shall be clearly defined and explained. The standards set in force in this connection by the bank must ensure rapid and efficient investigations so that in every case of suspected fraud, a decision can be taken quickly. A structure for control information and documentation must be set to ensure the protection of evidence and proper record keeping. The management shall have in place a notification structure for following-up investigations. SAMA must be notified of all significant fraud cases.

3-9-2 Guidelines
Operation staff and those responsible for the internal investigation must be provided with clear formal guidelines and procedures to ensure the treatment and investigation of fraud efficiently once discovered. The procedures for addressing and investigating fraud cases are very important particularly in the early stages, so as not to affect subsequent investigations. Staff training may be required, and a special training for selected employees may be needed. A record of all known cases of fraud discovered and investigations conducted must be maintained. Systems must be developed to follow up investigation and report its current status and results of its progress and continuous updates should be made. The management shall use reports to follow up the investigations. It is supposed that the senior management or the fraud control committee should receive programmed and regular reports on the status and progress of the investigations. The management plays a guidance role. It may not
3-9-2-1 Receiving a notification of alleged fraud

Appropriate structures of responsibility and channels of notification must be used (see the second basic condition entitled "Regulatory Framework and Structures of Responsibility" and the seventh basic condition entitled "Systems of Notification of Fraud"). The responsibilities of the person who receives a notification of suspected or discovered fraud should be defined clearly in the bank's guidelines for controlling and combating fraud.

The person who receives such notification or who discovers fraud or potential corruption shall mainly be responsible for recording all the details of the notification or suspicion as soon as possible in a confidential file referred to as a case report.

Details to be registered shall include the following (without any particular order of priority):

1. The date and time of the notification, incident or suspicion.
2. The name of the complaint (if applicable).
3. The name of the notifier, the incident or suspicion.
4. The details of communications.
5. The nature of the notification.
6. The time or period of alleged fraud.
7. The circumstances of the alleged crime.
8. The location of the alleged crime.
9. The name or names of the accused.
10. The address (es) of the accused.
11. The amount involved of the alleged fraud.

5. Any written notification received must be dated, stamped and dealt with in the same way as an oral allegation of fraud is addressed.

3-9-2-2 Initial Evaluation

The purpose of the initial evaluation of suspected fraud is to determine whether there is a ground for the notification or suspicion and the best measures to be taken.

Quick probe into all cases of alleged fraud shall be made. Suspected perpetrator may not be warned on the basis of the initial evaluation. Quick probe into all cases of alleged fraud shall be made. Suspected perpetrator may not be warned on the basis of the initial evaluation. It is worth mentioning that the accused has rights under the law. No action may be taken (such as investigating employees) without a prior consultation with the concerned members of the senior management and the Fraud Control Committee, Fraud Control Officer and other authorized staff, as applicable, pursuant to the fraud notification system at the bank.
Failure to follow the procedures in force for investigating fraud and interrogating employees involved may lead to impairing the disciplinary action and failure of any prosecution in the future. The confidentiality of the complainant and the recipient of the notification of fraud must be protected. The initial evaluation must be conducted after properly trained employees have collected available evidential information, provided that such collection of information should not disrupt any subsequent investigation. Based on the information available, necessary decision must be taken regarding the measures to be taken. The decision shall be one of the following conclusions: The complaint is groundless and no further measure is needed. The case must be referred to a higher director or to the Unit for Investigating Fraud Acts at the bank for further investigation. The case needs SAMA advice, the police or any competent legal authority to judge whether the crime has been committed or not. Decision on the case must be recorded together with the following: The reason for the decision. The article of the law according to which the decision is taken. Measures to be taken (if any). The identity of the person or external authority responsible for taking any subsequent measure. The name and position of the person who took the decision. The date of the decision. Possible options to conduct the investigation include the police, external auditors and investigators, and the bank's own staff or departments, such as Unit or Director of the Fraud Combat Unit, internal auditors or other internal audit units. Based on the size and nature of the alleged crime and the required expertise and resources available, it may be appropriate that a specific department makes the required investigation to form an opinion that a criminal act has been committed and the subsequent investigation be left to the police. These matters must be discussed with the external authorities concerned, such as SAMA and the police.

3-9-2-3 Updating of case reports
Responsibility must be clearly defined and the necessary regulations should be set to ensure the preservation of full and complete records of all fraud reports and cases. Report on a particular case must be updated if any significant change occurs in the case or on a quarterly basis, whichever is earlier. The bank shall be responsible for updating reports of

3-9-2-3-3-9-2-3 تحدث تقارير القضية:
تحديث المسؤولية بوضوح ووضع الأنظمة اللازمة لضمان المحافظة على السجلات الكاملة والمباشرة لجميع تقارير الاحتيال والحالات. تحديث تقارير القضية الخاص بقضية معينة عند حدوث تغيير هام في القضية أو كل ربع سنة، فيما أسبق. تغلى على عائق البنك مسؤولية تحديث تقارير القضية.
3.9-2-4 تطبيق خطة التحقيق:

عند اتخاذ قرار بالتعاون مع السلطات الخارجية على الأرجح بأن المبلغ المخالف في القضايا المحددة التي يجب إخطاها بالمحقق. يحدد المجالات التشغيلية والمعلومات التي سيشترك في التحقيق.

تحديد الخبرة المتخصصة أو الشروط المالية.

اللغة الموظفة للتحقيق وال-answer الزمنية اللازمة.

مواقع المراجعة ونقاطها الرئيسية وترتيب تقديم التقرير.

النتائج المتوقعة.

التحقيق الفعال والإشراف في عملية إخلاء كبير هو أمر معقد يقضي

خبرة متصورة وممارسة وقد تحتاج إلى الإبقاء على مستوى متقدم في المهارات والمهارة والتنظيمية والأخلاقية والمعايير المطلوبة.

التحقيق مع الشرطة، أن يكون التحقيق متعمدًا على سبيل المعرفة أو الخطأ أو الامتثال للقوانين.

بما أن التحقيق يتطلب مهاراتها بطريقة مستمرة.

بما أن التحقيق يتطلب مهاراتهم بطريقة مستمرة.

على قائم فريق التحقيق أن يعيد استخدام تكريم الحاجة إلى إشكال

العملاء والسماع المستقلة.

التحقيق الفعال والإشراف في عملية إخلاء كبير هو أمر معقد يقضي

خبرة متصورة وممارسة وقد تحتاج إلى الإبقاء على مستوى متقدم في المهارات والمهارة والتنظيمية والأخلاقية والمعايير المطلوبة.

التحقيق مع الشرطة، أن يكون التحقيق متعمدًا على سبيل المعرفة أو الامتثال للقوانين.

بما أن التحقيق يتطلب مهاراتها بطريقة مستمرة.

بما أن التحقيق يتطلب مهاراتهم بطريقة مستمرة.

على قائم فريق التحقيق أن يعيد استخدام تكريم الحاجة إلى إشكال

العملاء والسماع المستقلة.

التحقيق الفعال والإشراف في عملية إخلاء كبير هو أمر معقد يقضي

خبرة متصورة وممارسة وقد تحتاج إلى الإبقاء على مستوى متقدم في المهارات والمهارة والتنظيمية والأخلاقية والمعايير المطلوبة.

التحقيق مع الشرطة، أن يكون التحقيق متعمدًا على سبيل المعرفة أو الامتثال للقوانين.

بما أن التحقيق يتطلب مهاراتها بطريقة مستمرة.

بما أن التحقيق يتطلب مهاراتهم بطريقة مستمرة.

على قائم فريق التحقيق أن يعيد استخدام تكريم الحاجة إلى إشكال

العملاء والسماع المستقلة.

التحقيق الفعال والإشراف في عملية إخلاء كبير هو أمر معقد يقضي

خبرة متصورة وممارسة وقد تحتاج إلى الإبقاء على مستوى متقدم في المهارات والمهارة والتنظيمية والأخلاقية والمعايير المطلوبة.

التحقيق مع الشرطة، أن يكون التحقيق متعمدًا على سبيل المعرفة أو الامتثال للقوانين.

بما أن التحقيق يتطلب مهاراتها بطريقة مستمرة.

بما أن التحقيق يتطلب مهاراتهم بطريقة مستمرة.

على قائم فريق التحقيق أن يعيد استخدام تكريم الحاجة إلى إشكال

العملاء والسماع المستقلة.

التحقيق الفعال والإشراف في عملية إخلاء كبير هو أمر معقد يقضي

خبرة متصورة وممارسة وقد تحتاج إلى الإبقاء على مستوى متقدم في المهارات والمهارة والتنظيمية والأخلاقية والمعايير المطلوبة.

التحقيق مع الشرطة، أن يكون التحقيق متعمدًا على سبيل المعرفة أو الامتثال للقوانين.

بما أن التحقيق يتطلب مهاراتها بطريقة مستمرة.

بما أن التحقيق يتطلب مهاراتهم بطريقة مستمرة.

على قائم فريق التحقيق أن يعيد استخدام تكريم الحاجة إلى إشكال

العملاء والسماع المستقلة.

التحقيق الفعال والإشراف في عملية إخلاء كبير هو أمر معقد يقضي

خبرة متصورة وممارسة وقد تحتاج إلى الإبقاء على مستوى متقدم في المهارات والمهارة والتنظيمية والأخلاقية والمعايير المطلوبة.

التحقيق مع الشرطة، أن يكون التحقيق متعمدًا على سبيل المعرفة أو الامتثال للقوانين.

بما أن التحقيق يتطلب مهاراتها بطريقة مستمرة.

بما أن التحقيق يتطلب مهاراتهم بطريقة مستمرة.

على قائم فريق التحقيق أن يعيد استخدام تكريم الحاجة إلى إشكال

العملاء والسماع المستقلة.
the accused from his work location in the bank and put him under actual police custody to ensure the non-destruction of evidence or inflicting any harm on the bank or its systems.

3-9-2-5 Evidence Protection
It is very crucial to make sure that any form of evidence must not be lost or destroyed during the early stages. It must be ensured that the police has specialized necessary skills and equipment to preserve evidence and conduct judicial examinations.

A record of the locations from which evidence is obtained must be maintained.

The original documents must be protected and maintained in a safe place; such important documents must be replaced with copies thereof and kept in official files if necessary, so as to use the original in the conduct of any official procedure.

The original documents must not be marked with any distinctive signs.

Paper documents and slips of paper which may constitute evidence must not be handled, but they must be placed within a transparent plastic file permitting reading the document without handling with hands. The name of any person who handles such documents must be registered for use in the future.

Important evidence Information can be kept, for instance, on a printing tape, slip of paper or a copy book that looks empty. These items may provide valuable information to a trained specialist. Every possible effort must be made to protect these items from contamination.

Significant discussions with key officials must be documented.

Important evidence could be found in the office of the accused, his file safe, closed drawer, briefcase or in his car. Before inspecting these places or banning access to them, the bank’s legal affairs department must be consulted about the legal consequences of such action and for reaching the conclusion that the accusation was not based on any ground. If computers were used to commit a fraudulent act, an expert must be consulted before making any attempt to protect the data stored in the computer or other storage media concerned, and to analyze or even access them. Negligence in taking proper precautionary measures may result in creating destructive or self-destructive programs that could damage the computer hardware or destroy important evidence.

When assessing aspects of computer fraud, priorities of the investigation team must be to protect the hardware and the network, which may have been accessed by the accused, in order to ensure continuity of operations and services and protect storage media and codes and other items that may be
used as evidence. It may be necessary to seek the help of computer experts and other internal and external specialists to set and implement protection controls.

When the data manager, systems analyst, network specialist or information technology specialist is highly skilled, it is particularly important to make sure not to give such a person any advance warning about the investigation. After discussions with efficiently qualified employees, all rights of entry and access to all systems must be withdrawn as a first priority.

3-9-2-6 Recovery of the proceeds of fraud
Recovery of all losses resulting from fraud must be pursued, whether punitive measures have been taken or not. Control systems must be reassessed after the fraudulent act to avoid its recurrence. Recovering the proceeds of fraud and other losses can be pursued through criminal prosecution or through other channels, such as administrative or disciplinary measures.

3-10 Ninth Basic Condition: Code of Conduct and Disciplinary Measures

3-10-1 Introduction
Banks shall develop an appropriate code of conduct and circulate it to employees, suppliers, customers and the public in general. A clear message must be sent that fraud will not be tolerated with and its perpetrators shall be subject to disciplinary measures. In this regard, the code of conduct will constitute a starting point, supported by specific standards and policies which cover all employees and create a climate of ethical conduct inside the bank. These standards must extend to the hired employees, private contractors, suppliers, consultants and all parties dealing with the bank and its functions.

3-10-2 Guidelines
Banks shall develop proper code of conduct and distribute it to employees, suppliers, customers and the public in general. The code of conduct shall cover all categories of staff at the bank. This code of conduct must be extended to the bank's contracted employees, private contractors, suppliers, consultants and agents, and any person dealing with the bank or with its functions. Different codes of conduct or minimum codes of conduct and disciplinary procedures can be set to cover the bank as a whole. However, such codes of conduct must be applicable to particular situations in certain departments or sections.
3-10-2-1 Codes of Conduct
Setting and distributing codes of conduct could help in identifying the behavioral and ethical standards required at the bank. They must reflect and describe the integrity of the bank’s employees, their ethical values, and competence; personal and professional behavior expected of all staff; the philosophy of the bank and its operational system; the means on basis of which the management of the bank determines powers and responsibilities, and the way in which it develops the competence of its members; attention paid by the board of directors to these standards and its guidance thereto.

The message contained in the Code of conduct must be reinforced by using other forms of official documents, such as employee's booklet and procedures (including a booklet manual on controlling and combating fraud) with necessary details, newsletters and circulars which can be used to effectively promote these standards and strengthen them regularly.

3-10-2-2 Disciplinary Standards
The employee's booklet must specify disciplinary measures to be taken by the bank against employees who are convicted of fraud. A head of a department may not generally accept the resignation of an employee under investigation because of his dishonest behavior or any other immoral behavior that requires his dismissal from service. Although the resignation of such an employee may be considered as a means for saving time and cost involved in the dismissal from service, there is a possibility that he may continue practicing fraudulent acts while working at another institution or firm. This may cause embarrassment to the bank that allowed this person to resign, or file a law suit against the bank.

3-10-2-3 Standards Applicable to Temporary Staff and Employees of External Outsourcing Entities
The same standards applicable to the management of the bank and its staff must apply to temporary staff and other employees of external entities with which the bank is outsourcing. The entities must realize the bank's ethical aspirations that they are expected to meet. For optimal benefit from outsourcing with the external entities, banks must establish management and control systems that would control costs and reduce fraud, waste of resources and mismanagement as much as possible.

When it depends on external human and technical resources to perform certain services, the bank shall make sure to monitor the employees of contracted firms and evaluate their performance to determine if there is a risk of fraud and take necessary measures to combat and detect such fraud.

3-10-2-3 Codes of Conduct
3-10-2-4 Standards Applicable to Temporary Staff and Employees of External Outsourcing Entities
3-10-2-5 Disciplinary Standards
3-10-2-6 Standards Applicable to Temporary Staff and Employees of External Outsourcing Entities
3-10-2-7 Codes of Conduct
3-10-2-8 Standards Applicable to Temporary Staff and Employees of External Outsourcing Entities
3-10-2-9 Disciplinary Standards
3-10-2-10 Standards Applicable to Temporary Staff and Employees of External Outsourcing Entities

The risk assessing process aimed in particular at determining the risk of fraud involved in a particular contract represents a part of risk management described in the third basic condition under the title "Assessing the Risk of Fraud". Once risks are identified, managers shall develop strategies applicable to that contract.

Strategies aimed at reducing risks associated with outsourcing must be set in full details and must include specific arrangements for guidance and control to ensure sound financial management, effective accounting and clear courses for accounts audit.

In order to mitigate risks, managers should have the necessary skills or receive the necessary training to take appropriate decisions concerning the issues involved in outsourcing.

In outsourcing with external parties, the legal department at the bank must ensure that procedures, guidelines and instructions of SAMA in this regard are taken into consideration.