مؤسسة النقد العربي السعودي

إدارة التفتيش البنكي

Saudi Arabian Monetary Agency

Banking Inspection Department

دليل مكافحة الاختلاس والاحتيال المالي

وإرشادات الرقابة

1429هـ

Manual of Combating Embezzlement & Financial Fraud & Control Guidelines

2008

مؤسسة النقد العربي السعودي
ص . ب 2992
الرياض 11169
المملكة العربية السعودية
الهاتف 4662440- 1- 966+
الفاكس 4662865- 1- 966+

The Saudi Arabian Monetary Agency
P.O. Box 2992
Riyadh 11169
Kingdom of Saudi Arabia
Tel No +966-1-4662440
Fax No +966-1-4662865

Contents

جدول المحتويات

1- 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.

1- **تمهيد :**

يشمل هذا الدليل ضوابط إرشادية عامة من الواجب أخذها بالاعتبار عند تصميم أو تقييم السياسة الخاصة بمكافحة ومراقبة عمليات الاختلاس و الاحتيال المالي في البنوك التجارية العاملة في المملكة العربية السعودية.

وتعتبر هذه الضوابط مكملة للتعليمات السابقة الصادرة عن مؤسسة النقد فيما يخص مكافحة الاختلاس و الاحتيال المالي ، إلا أنها ذات طابع أكثر شمولية، وتتضمن ضوابط تهدف إلى مكافحة الاختلاس و الاحتيال المالي، ولهذا كان تعديل عنوان الدليل ليعكس هذا الاتجاه.

أعدت المؤسسة هذا الدليل لمساعدة المدراء وكبار المسئولين في البنوك على تقييم مخاطر حدوث الاحتيال في البنوك وكيفية التصدي لمثل هذه العمليات وذلك عن طريق إستراتيجية عامة لمكافحة ومراقبة عمليات الاحتيال بما يناسب كل بنك على حده . تستند هذه التعليمات الإرشادية إلى تسعة شروط أساسية لاتخاذ إستراتيجية فاعلة لمكافحة الاحتيال والكشف عنه والسيطرة عليه. لكل شرط أساسي مقدمة موجزة وعامة تليها ضوابط إرشادية محددة ترمي لمساعدة البنوك في تطبيق هذه الضوابط .

وبهدف مواكبة تطور الممارسات الهادفة لمكافحة ومراقبة عمليات الاحتيال سوف يتم تحديث هذه الضوابط الإرشادية من وقت لآخر.

وبصفة عامه فإن هذه الضوابط تهدف إلى توفير دليل عملي للتقييم الذاتي من قبل البنوك لتطبيق إستراتيجية شاملة لمكافحة الاحتيال وكذلك كبداية مشروع للاهتداء به.

و ينبغي استعمال هذا الدليل مع تعليمات مؤسسة النقد العربي السعودي الإرشادية وتعاميمها الأخرى ذات الصلة الواردة في المقدمة. و يعتبر الدليل ضروري لتطوير برنامج متكامل لمكافحة ومراقبة عمليات الاحتيال بحيث يكون من ضمن مهام إدارة المخاطر التشغيلية الشاملة و مخاطر العمليات ومن ضمن نظام الرقابة الداخلية لدى البنك.

ويعتمد نجاح ضوابط مكافحة ومراقبة عمليات الاحتيال في الأساس على مدى التزام مجلس الإدارة والإدارة التنفيذية للبنك بتطبيق تلك الضوابط، إضافة إلى التوقيت الجيد وتوفير الموارد المالية والبشرية اللازمة. وبغرض تحقيق النجاح في تطبيق عملية مكافحة الاحتيال، فإنه لابد للإدارة أن لا ينحصر عملها على الإشراف والقيادة فحسب بل أن تكون القدوة في ممارسة تطبيق أعلى المعايير الأخلاقية والسلوك المهني الملائم. لهذا فان هذه الضوابط موجهة بشكل مباشر لأعضاء مجالس إدارات البنوك وكبار المسئولين فيها بالإضافة إلى المجموعات الوظيفية المختلفة واللجان والأفراد الذين يتولون مهام محددة تتعلق بإستراتيجية مكافحة ومراقبة عمليات الاحتيال.

2- Introduction
2-1 Overview

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- مقدمة :

2-1 لمحة عامة :

الاحتيال هو واحد من التحديات التي تواجه المنشآت المالية أو المصرفية ، فهو يعيق الأداء ويهدر الأموال والموارد النادرة ويلحق الأذى بالمنشأة وبسمعتها وبقدرتها التنافسية. وقد يتخذ الضرر أشكالاً عدة غير الخسارة المالية بحد ذاتها مهما بلغت قيمتها. فالضرر الأكبر قد يكون ذلك الذي يلحق بأداء المنشأة وسمعتها ومصداقيتها وثقة السوق والجمهور بها وفي نهاية المطاف قد يؤدي إلى تعريضها لمخاطر متعددة.

والمشكلة كبيرة بكل المقاييس ويبدو أنها لا تقتصر على أي منشأة بعينها في القطاع الخاص سواءً كانت منشأة مالية أو صناعية أو خدمية ، إضافة إلى ذلك أن الاحتيال يتكيف مع المتغيرات التي قد تطرأ على أي قطاع ، فبالرغم من آليات التدقيق الداخلي والمراقبة والتقصي وشروط مراجعي الحسابات الخارجيين المستقلين وقواعد السلوك المهني يستمر حدوث الاحتيال.

ويصعب في الغالب استرداد الأموال المهدرة بسبب نشاطات الاحتيال، وفي كثير من الأحيان يكون هذا الأمر مستحيلاً. لذلك تكون برامج مكافحة ومراقبة عمليات الاحتيال أقل كلفة وأكثر فعالية من محاولات استرداد تلك الأموال المختلسة.

وبالرغم من ذلك فإن هناك عدد من البنوك والمنشآت المالية قد تلجأ للتأمين لحماية نفسها ضد المخاطر التشغيلية الناتجة عن أحداث مثل الاختلاس والاحتيال المالي من قبل الموظفين ، ومع ذلك فإنها لا تستطيع أن تعتمد كلياً على التأمين كوسيلة للتخفيف من المخاطر التشغيلية، فالتأخير في الدفع والطعون النظامية بالشروط التعاقدية تؤكد بأن التأمين لا يوفر التغطية المثالية، أضف إلى ذلك فان النتائج السلبية للمطالبات المتصلة بالاحتيال ستؤدي إلى ارتفاع أقساط التأمين خاصة عندما تكون قوى السوق تتجه نحو تصعيد أسعار التأمين حتى للبنوك التي لها سجل جيد في مثل هذه العمليات.

وبالنسبة لكفاءة رأس المال النظامية للمخاطر التشغيلية التي اقترحتها لجنة بازل ، سيطلب من البنوك مستقبلاً أن تجنب مخصصات نظامية من رأس المال للمخاطر التشغيلية. وإضافة إلى تحمل خسائر مالية مباشرة وأقساط تأمين متصاعدة فان البنوك ذات السجل الضعيف في مكافحة الاحتيال ستجد أن نتائجها المالية قد تتأثر سلباً نتيجة لزيادة متطلبات كفاية رأس المال النظامية، وتقع على عاتق الإدارة التنفيذية للبنوك السعودية مسؤولية التأكد من أنها تطبق إستراتيجية لمكافحة ومراقبة عمليات الاختلاس و الاحتيال المالي. ونظراً للتقدم التقني السريع وانتشار الجريمة المنظمة على نطاق عالمي فإنه من الضروري مراجعة هذه الإستراتيجية بشكل دوري وتحديثها استجابة

للمخاطر الجديدة والتقنيات التي يستخدمها المحتالون، وعليه فإن هذه التعليمات الإرشادية تهدف إلى مساعدة كبار المسئولين التنفيذيين في تنفيذ هذه الاستراتيجيات.

2-2 تعريف الاحتيال:

التعريف البسيط للاحتيال هو أية ممارسة تنطوي على استخدام الخداع للحصول المباشر أو غير المباشر على شكل من أشكال الاستفادة المالية لمرتكب الجريمة، أو تسهيل ذلك لغيره لتؤدي إلى شكل من أشكال الخسارة للطرف الذي تعرّض للاحتيال. وغالباً ما تتصل الخسارة الفعلية الناتجة عن الاحتيال في البنوك بالموجودات السائلة مثل النقد والأوراق المالية .

وليس من الضروري أن يقتصر الاحتيال على المنافع النقدية والمادية. فتعريف الاحتيال الوارد في المراجع هو "التحريف المتعمد للحقيقة لأغراء أحدهم بالتنازل عن شيء ذي قيمة أو عن حق قانوني". ويشمل هذا التعريف الكسب المالي إلى جانب منافع أخرى مثل حق الدخول أو الحصول على معلومات يمكن اكتسابها بالخداع أو بأي سلوك آخر غير شريف، وسواء كانت الخسارة مادية أو كانت تتصل بشيء غير ملموس مثل حقوق الملكية الأدبية، فغالباً ما ينطوي الاحتيال على خسارة للبنك أو للمساهمين فيه أو للعملاء ومحاولة إخفاء تلك الخسارة.

ويمكن أن يشمل الاختبار الأساسي للاحتيال الأسئلة التالية:

* هل هناك خداع للمنشأة؟
* هل كان الفعل غير شرعي؟
* هل نتج عن ذلك استفادة أو منافع مالية لصالح شخص لا يستحقها ؟
* هل تمت المحاولة للقيام بأي من ما ورد في الأسئلة السابقة ؟

ويجب التمييز بين الاحتيال من داخل البنك والاحتيال من خارج البنك وتبيّن الدراسات التي أجريت على مؤسسات دولية باستمرار أن مرتكبي الاحتيال في معظم الأحوال هم من الموظفين ، بمساعدة أو بدون مساعدة شركاء من الخارج، يدفعهم إلى ذلك عادة انتهاز الفرص والجشع والانتقام والحاجة لنقد سريع لدعم طراز معين من المعيشة ومشاكل مالية شخصية وعدم الرضا أو الولاء والضغط العائلي والحاجة لتسديد الديون.

وتتشابه البنوك من حيث ما تواجهه من احتيال في معظم دول العالم حيث أن معظم الخسائر تأتي نتيجة أعمال احتيالية من جانب الموظفين ، وربما يشكل اختلاس النقود أكثرها شيوعاً ، وبصورة خاصة اختلاس النقود والشيكات السياحية من الفروع ومكائن الصرف الآلي. ولابد من الإشارة إلى أن حالات اختلاس النقد تنطوي على مبالغ غالباً

by fraudsters. These guidelines aim at helping senior officials to carry out this task.

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

ما تكون زهيدة. في حين أن حالات الاحتيال عن طريق الدفع أو التحويل الالكتروني أقل عددا نسبيا ولكنها تنطوي عادة على خسائر مالية أكبر.

ومن المعلوم تاريخياً أن معظم الخسائر الناتجة من عمليات الاحتيال في البنوك تكون بسبب أشخاص يعملون لدى تلك البنوك في جميع المستويات الوظيفية ، لذلك يتعين على أية إستراتيجية تهدف إلى مكافحة الاحتيال أن تركز بصورة أساسية على ما يسمى بالاحتيال "في مكان العمل". في الوقت ذاته، فان مفهوم الاحتيال لا يجوز أن يتجاهل خطر الاحتيال الخارجي، أو ما يشار إليه أيضاً باحتيال العميل.

والاحتيال الخارجي يرتكبه أشخاص من خارج البنك (عادة ما يكونوا مجرمين محترفين) وغالبا بمساعدة ومعرفة أشخاص من داخل البنك.

ولفهم الاحتيال بصورة صحيحة، علينا أن ندرك أن أعمال الاحتيال يرتكبها أشخاص هم موضع ثقة. وهذا ما يفسر طول المدة في اكتشاف الاحتيال ولماذا عند اكتشاف المرتكب، يقر زملاؤه أن شكوكاً كانت تساورهم لبعض الوقت لكنهم كانوا يشعرون بعجزهم عن القيام بأي عمل قد يساعد على اكتشاف هذه العمليات في وقت مبكر.

ويمكن اعتبار الاحتيال كجزء هام جداً، من القضية الأوسع المعروفة باسم الفساد. وينطوي الفساد بصورة عامة على أعمال غير صالحة أو اغفالات أو سوء استخدام النفوذ أو المراكز أو سوء استخدام المعلومات. ومع أن هذه الإرشادات يمكن إتباعها لمعالجة الفساد بصورة عامة، إلا أنها تركز تحديداً على قضية الاحتيال ولا تدعي معالجة جميع أبعاد الفساد الممكنة.

2-3 الاحتيال وغسل الأموال :

غسل الأموال هو التعبير الشائع المستعمل في وصف الوسائل التي يتم من خلالها معالجة "المال غير الشرعي" الناتج عادة عن أنشطة إجرامية عبر النظام المالي ليصبح "مالاً شرعياً" بحيث لا يمكن اقتفاء أثر الشخص الذي باشر العملية أو المصدر الإجرامي للأموال.

وفي الواقع العملي يسير الاحتيال وغسل الأموال جنباً إلى جنب. وعند نقطة معينة من المحتمل أن يطور المحتال الذكي حاجة لغسل عائدات نشاطاته الإجرامية. أما غاسلو المال فيلجئون بدورهم إلى الاحتيال لإخفاء مصدر وملكية أموالهم ومحاولاتهم لإعادة تدوير المال في الاقتصاد.

وبما أن الاحتيال وغسل الأموال غالباً ما يرتبطان ويتواصلان معاً، فلا بد إذا من وجود درجة من التداخل بين الاستراتيجيات الرامية إلى مكافحة هذه الأنواع من الأنشطة. فالقواعد الصادرة عن مؤسسة النقد لمكافحة عمليات غسل الأموال وتمويل الإرهاب تهدف تحديداً إلى مكافحة غسل الأموال وتمويل الإرهاب عبر البنوك السعودية. لذلك

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. This explains why it often takes a long time before discovering fraud, and why when the perpetrator is caught his colleagues admit that they were entertaining suspicion about him for a while; yet they were unable to do anything that might help detecting such acts at an earlier time.

Fraud may be considered as an integral part of the widely-spread phenomenon known as "corruption", which in general involves illegal actions; negligence; misuse of power, position, or information. Though these guidelines can be followed to address corruption in general, yet they mainly focus on fraud acts, and it cannot be alleged they can be used for addressing all possible implications of corruption.

2-3 Fraud & Money- Laundering

Money–laundering is the common expression for describing the methods through which "dirty money", which usually results from criminal acts, is transferred through the financial system so that it becomes "clean money" and the person committing the crime or the criminal source of money can not be traced.

In reality, fraud and money-laundering go hand in hand. At some point, it is likely that the fraudster develops a way to launder the proceeds of his criminal activities. Money–launderers commit fraud to hide the source and ownership of their funds and try to recycle money in the economy.

Since fraud and money-laundering are often interrelated and connected together, strategies aimed at combating such types of acts are inevitably overlapped. The control guidelines issued by SAMA to combat money-laundering and finance of terrorism operations via the banking system aim at combating money-laundering through Saudi banks. Therefore, the money-laundering issue is in not

استثني موضوع غسل الأموال من نطاق هذه الإرشادات مع أن بعض تدابير مكافحة الاحتيال المدرجة هنا قد تجد كما ورد سابقاً تطبيقاً موازياً في الجهود الرامية إلى مكافحة غسل الأموال وتمويل الإرهاب.

2-4 عينة من عمليات الاحتيال :

هناك عدة أمثلة من الاحتيال المصرفي منها :

اختلاس النقد والموجودات الثمينة الأخرى.

- تزوير أو تحريف المستندات بما في ذلك طلبات التوظيف والفواتير والشيكات وشهادات الأهلية أو التأهيل أو مستندات الهوية ،أو بطاقات الصرف الآلي ،أو البطاقات الائتمانية.
- تزوير التواقيع والأختام .
- تزييف الأوراق النقدية .
- تغيير أحد أو كل أركان مكونات الشيك.
- سرقة بطاقات الصرف الآلي أو بطاقات الائتمان واستعمالها بطريق غير شرعية.
- إدخال تعليمات وبيانات غير سليمة من خلال الحاسب الآلي .
- سوء استخدام المعلومات وتسريبها بطرق غير شرعية .
- تحويل أموال لعملاء وهميين أو موظفين أو باعة.
- قبول الرشاوى أو الهدايا أو العمولات السرية لمنح عقد أو تجاهل الإجراءات المتخذة وحالات عدم الالتزام أو كدافع لتقديم منافع بما في ذلك الوصول إلى معلومات سرية.
- الحصول عن طريق الاحتيال على منافع أو مستندات لا يحق للمستلم أن يحصل عليها.

2-5 دور التقنية :

أثبتت التقنية الحديثة في القطاع المصرفي أنها سلاح ذو حدين. فمن ناحية استفادت جهود مكافحة الاحتيال بشكل واضح من التقنية الحديثة إذ أن الانتقال من النظام النقدي إلى نقل الأموال الكترونيا، على سبيل المثال، قد خفض من أخطار اختلاس النقود لانخفاض حيازة النقود. كما أن تطوير وسائل وأدوات لاكتشاف الاحتيال يعود الفضل فيه إلى أدوات التقنية المتطورة.

ولكن من ناحية أخرى فقد برع المحتالون باستخدام أحدث التقنيات لتعزيز قدراتهم. ويمكن القول أن لا شيء قد سهل الاحتيال أكثر من الانتشار الواسع لأجهزة الحاسب الآلي زهيدة الثمن وعالية القدرة والمتوفرة بسهولة وما يتصل بها من تقنيات أخرى. فتقنيات المستندات الحالية مثل الماسحات البصرية وطابعات الليزر والناسخات والبرامج المختلفة قد سمحت بأعمال تزوير يصعب جداً اكتشافها. فوسائل تزوير الشيكات البسيطة في السابق قد حل مكانها أعمال تزوير عالية الجودة لجميع الأوراق المالية القابلة للتداول بما في ذلك الشيكات

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.

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

وخطابات الاعتماد وأذونات الخزينة والسندات. وبما أن البنوك السعودية قد تقدمت كثيراً في الفترة الماضية في إدخال النظام التقني على أنظمتها من الأرجح أن ينخفض عدد أعمال تزوير المستندات، في حين أن مستوى التزوير التقني المتطور وقيمته النقدية سيصبح الأرجح.

كما أن التقنيات الحديثة قد سمحت بتزييف العملات وبطاقات الائتمان بشكل واسع، وهو نشاط معروف لدى عصابات الجريمة المنظمة. فعمليات تزييف العملات الرئيسة ، بصورة خاصة، تمارس على المستوى الدولي بالتعاون مع عصابات غسل الأموال.

ولقد أدّت التقنيات الحديثة، إضافة إلى خطر الاحتيال التقليدي المرتبط بعمليات (Insider Trading) إلى ارتفاع مخاطر التعرض للخسائر المالية. فعند قيام أحد موظفي البنك بتعديل حالة مديونية بصورة احتيالية أو عند قيام أحد الوسطاء بإجراء صفقات غير معتمدة أو بتجاوز حدود الصفقة فان كل منهما يعرض البنك إلى خسائر مدمرة محتملة في فترة قصيرة من الوقت.

أن التحول إلى النشاط المصرفي عن طريق الانترنت يعرض البنوك كذلك إلى مخاطر جديدة. فالمحتالون مطلعون على أحدث التقنيات بعمق وعلى نقاط الضعف الكامنة في إجراءات الرقابة الداخلية لدى البنوك وهم يمثلون خطراً متنامياً من مخاطر الجريمة الالكترونية ("Cyber Crime").

ومن غير المتوقع أن تواكب المعلومات حول الجريمة الالكترونية الواردة في هذه الإرشادات التقدم السريع للتطور التقني. لذلك يتوجب على البنوك أن تظل مطلعة على أحدث التطورات التقنية التي يستخدمها المحتالون وعلى أحدث الوسائل لاكتشاف ومراقبة ومكافحة الاحتيال. ولهذه الغاية ينبغي استمرار تطوير الأنظمة والإجراءات الداخلية لرصد وتحليل اتجاهات الاحتيال ووسائل مكافحته وإيجاز هذه المعلومات الهامة وتوزيعها على موظفي البنك. وتتضمن خطة مكافحة ومراقبة عمليات الاحتيال الواردة في هذه الإرشادات عدداً من الاقتراحات بهذا الشأن.

2-6 تعاميم مؤسسة النقد العربي السعودي والخطوط الإرشادية المساندة :

أصدرت المؤسسة عدداً من التعاميم بشأن الاحتيال. ويمكن الحصول على هذه التعاميم في "دليل تعاميم ساما" في القسم 120 بعنوان "الجرائم الاقتصادية". الجدول التالي يصف بإيجاز الأقسام الفرعية للتعاميم المتصلة بالجرائم الاقتصادية في هذا الدليل:

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 the 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 theses 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:

القسم	موضوع التعميم
1/120	إبلاغ سلطات الأمن بأعمال الاحتيال
2/120	إرشادات لمكافحة الابتزاز المالي والاحتيال
3/120	إرشادات لمكافحة غسل الأموال
4/120	محاولات تزييف العملة الوطنية وجهود مكافحتها
5/120	محاولات تزييف العملات الأجنبية وجهود مكافحتها
6/120	محاولات لتزوير المستندات وجهود مكافحتها
7/120	أعمال احتيال بنكي أخرى
8/120	لجنة تسوية المنازعات المصرفية
9/120	لجنة مكافحة الاختلاس والاحتيال المالي
10/120	لجنة خزينة البنك
11/120	الدعاوى والمنازعات البنكية
12/120	عد العملات ومكائن الفحص

Section	Circular Subject
120/1	Notifying authorities concerned of fraud operations
120/2	Guidelines to combat financial embezzlement and fraud
120/3	Guidelines to combat money-laundering
120/4	Attempts of forging the national currency and efforts to combat them
120/5	Attempts of forging foreign currency and efforts to combat them
120/6	Attempts of forging documents and efforts to combat them
120/7	Other banking fraud operations
120/8	Committee for Resolution of Banking Disputes
120/9	Committee for Combating Embezzlement and Financial Fraud
120/10	Bank Treasury Committee
120/11	Banking complaints and disputes
120/12	Currency counting and examination machines

كما أصدرت المؤسسة عدداً من الإرشادات والكتيبات المساندة التي يتوجب قراءتها بالتزامن مع هذه الضوابط. وهي تشمل ما يلي:

دليل إرشادات مكافحة عمليات الاختلاس والاحتيال المالي

إدارة المخاطر التشغيلية عن طريق برامج التأمين.

معايير دليل الأمن للشركات.

إرشادات الرقابة الداخلية للبنوك التجارية.

المعايير المحاسبية للبنوك التجارية.

الشروط الدنيا للأمن الفعلي.

الشروط الدنيا لأنظمة الأمن.

قواعد فتح الحسابات والقواعد العامة لتشغيلها.

قواعد مكافحة غسل الأموال وتمويل الإرهاب .

تعليمات عمل حراس الأمن.

إجراءات حماية النقد أثناء النقل.

إرشادات لحماية ومراقبة نشاطات غسل الأموال عبر النظام البنكي.

إرشادات بشأن أمن الانترنت البنكي.

3- خطة مكافحة الاحتيال :

3-1 مقدمة :

من الضرورة أن يقوم كل بنك بوضع خطة متكاملة لمكافحة الاحتيال لمعالجة جميع جوانب الاحتيال. وتقترح هذه التعليمات تسعة شروط أساسية لتطوير خطة فاعلة لمكافحة الاحتيال لدى البنوك السعودية، وذلك بالاستناد إلى مراجعة واعتماد أفضل الممارسات الدولية في هذا المجال. وهذه الشروط الأساسية التسعة المقترحة هي كالتالي:

الأول: إستراتيجية مكافحة الاحتيال وسياسة الرقابة .

الثاني: الإطار التنظيمي وهيكلية المسؤولية .

الثالث: تقييم مخاطر الاحتيال .

الرابع: نشر الوعي بشأن الاحتيال .

الخامس: إجراءات المراقبة .

السادس: الرقابة والمتابعة.

السابع: أنظمة الإبلاغ عن الاحتيال.

الثامن: معايير التحقيق.

التاسع: معايير السلوك والتأديب

هذه الشروط والتعليمات الإرشادية هي عامة لا تفصيلية تتضمن قائمة بالأمور التي تحتاج للمعالجة بعمق من قبل أي بنك حسب ظروفه الخاصة. وتقع على عاتق البنك مسؤولية تطوير الإجراءات والمعايير والأنظمة والعمليات اللازمة لتطبيق هذه الشروط بصورة فاعلة ومتابعتها كجزء من حملة مستمرة يشنها البنك بكامله لمكافحة الاحتيال.

جوهر أسلوب مكافحة الاحتيال هو الاقتناع بأهمية إدارة المخاطر. فباستخدام تقنيات الإدارة تستطيع أن تحدد بوضوح معظم نقاط الضعف

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.
Manual of company security standards.
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.
Eight: 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 operations 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

في الضوابط وأن تتخذ التدابير اللازمة لإصلاح آليات المراقبة الضعيفة أو إدخال تقنيات إضافية.

تناقش الأجزاء التالية الشروط الأساسية التسعة كل على حده بحيث يبدأ كل جزء بمقدمة عامة موجزة تليها إرشادات محددة تهدف إلى مساعدة البنوك في جهودها لمعالجة احتياجاتها الخاصة.

3-2 الشرط الأساسي الأول: إستراتيجية مكافحة الاحتيال وسياسة الرقابة:

3-2-1 مقدمة :

يتعين على كل بنك أن يكون لديه سياسة مكتوبة شاملة ومتكاملة لمكافحة الاحتيال ومراقبته مع تفاصيل المراقبة لمكافحة الاحتيال والفساد. ويجب أن ترسم هذه السياسة كافة التدابير والإجراءات الصالحة للبنك المعين، إلى جانب سلسلة واسعة ومكملة من التدابير المضادة للاحتيال. ويجب أن تتبنى هذه السياسة أسلوب إدارة المخاطر لمكافحة ومراقبة الاحتيال، كما يجب أن يكون الغرض الرئيسي لهذه السياسة هو نشر الوعي والالتزام بين الموظفين، وان تحدد من هو المسئول في البنك عن مكافحة ومراقبة الاحتيال وعن تطبيق مختلف جوانب خطة مكافحة ومراقبة الاحتيال. ومن أجل تقييم فعالية الخطة يجب أن تخضع هذه الخطة للمتابعة والتقييم من الداخل والخارج.

3-2-2 الإرشادات :

1- على البنك أن يضع سياسة مكتوبة لمكافحة الاحتيال ومراقبته ويتم توزيعها على موظفيه.

2- تتضمن هذه السياسة مراقبة البنك للاحتيال ومكافحة الفساد وأن تضع الأهداف وأن تجمع السياسات القائمة والإجراءات التي تتصل بمكافحة الاحتيال والفساد .

3- يمكن أن ترد السياسة في وثيقة واحدة أو في مجموعة من الكتيّبات والتوجيهات والتعاميم والإرشادات توضح بمجملها عناصر إستراتيجية البنك.

4-تقوم السياسة على أساس تحليل مخاطر البنك من حيث بيئته الداخلية والخارجية وأن تتبنى أسلوب إدارة المخاطر بشأن مراقبة الاحتيال (يغطي هذا الجانب الشرط الأساسي الثالث بعنوان "تقييم خطر الاحتيال").

5-تكون السياسة شاملة وأن تغطي العناصر الحيوية للبنك ونشاطاته.

6-تكون السياسة متكاملة دون أي تضارب بين العناصر المستقلة.

7-تغطي السياسة بحدها الأدنى الشروط الأساسية المذكورة في 3-1.

8-تحدد سياسة مكافحة الاحتيال بالتفصيل أعضاء لجنة مكافحة

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

الاحتيال ونطاق عملها وأغراضها. المؤلفة من موظفين رئيسيين من مختلف أقسام البنك مسئولة عن تطوير تلك السياسة وتطبيقها وتنسيقها (راجع الشرط الأساسي الثاني بعنوان "الإطار التنظيمي وهيكلية المسؤولية").

9-على المسئولين التنفيذيين أن يكونوا القدوة بالتصرف بنزاهة والتقيد بروح ونصوص سياسة مكافحة الاحتيال ومراقبته. كما يجب أن يدركوا بأنهم مسئولين وخاضعين للمحاسبة في إيجاد مناخ أخلاقي والمحافظة عليه مما يؤدي إلى إحباط الاحتيال وتشجيع الإبلاغ عن أي خرق للمعايير المقبولة.

10-رصد ما يكفي من العناصر البشرية والموارد الأخرى لضمان نجاح سياسة مكافحة ومراقبة الاحتيال. فالالتزام الواضح من كبار المسئولين من حيث الوقت ورصد الموارد، يساعد في إرسال إشارة واضحة إلى الموظفين بان الإدارة لن تتهاون في مكافحة الفساد.

11-على جميع الموظفين أن يعوا مسؤولياتهم المتعلقة بمكافحة الاحتيال والكشف والإبلاغ عنه والتحقيق بشأنه (راجع أيضاً الشرط الأساسي الرابع بعنوان "نشر الوعي بشأن الاحتيال).

12-أنه من الملائم إشراك الجهاز التشغيلي في وضع صيغة سياسة مكافحة الاحتيال لتحديد أين توجد فرص الفساد وكيف يمكن تقليصها للحد الأدنى.

13-من الأهمية بمكان إطلاع الجهاز التشغيلي باستمرار على تطورات السياسة وتطبيقها والإنجازات والمنافع لتعزيز الالتزام بأغراض تلك السياسة على أوسع نطاق.

14-يساعد العمل الجماعي ونشر الثقافة التنظيمية البنوك على الاستفادة من الخبرات والأفكار المجمعة.

15-تكييف وتحديث سياسة مكافحة ومراقبة الاحتيال بحيث تعكس التغييرات في البنك وفي بيئته التشغيلية . ولهذا الغرض يتم مراجعة السياسة دورياً كل سنتين مثلاً أو عند حدوث تغييرات في البيئة التشغيلية تؤدي لإضعاف قدرة تلك السياسات على مكافحة ومراقبة الاحتيال وأيضاً لاستعراض قدرتها على تلبية الأغراض المعاد تقييمها.

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 الشرط الأساسي الثاني: الإطار التنظيمي وهيكلية المسؤولية :

3-3-1 مقدمة :

يجب تطوير إطار تنظيمي شامل وفعّال وهيكلية مسؤوليات لتنفيذ سياسة مراقبة الاحتيال الشاملة التي يعتمدها البنك، يتضمنها تنفيذ أنظمة مراقبة داخلية سليمة. وينبغي تكوين لجنة لمراقبة الاحتيال لوضع السياسة وتنسيق ومتابعة تنفيذها وتوفير المساندة اللازمة لها. و إشراك جميع مستويات الإدارة في تنفيذ هذه السياسة.

3-3-2 الإرشادات :

1-تحديد المسؤولية التنظيمية لإستراتيجية البنك الشاملة لمكافحة الاحتيال ولكل عنصر من عناصرها بكل وضوح وإبلاغ إدارة البنك وموظفيه بكل ذلك.

2-ينبغي أن تكون هناك لجنة مستقلة كما ذكر في 3-3-1 معنية بمكافحة ومراقبة الاحتيال لدى البنك، كما نوصي بالأمور التالية:

تكون مهمة لجنة مراقبة الاحتيال هي وضع وتنسيق ومتابعة سياسة الكشف عن الاحتيال والتحقيق بشأنه.
تحديد مسؤولية مراقبة الاحتيال بكل وضوح.
تنفيذ هيكلية واضحة للإبلاغ عن الاحتيال.

3-توثيق أدوار ومسؤوليات جميع الموظفين بوضوح في سياسة مكافحة ومراقبة الاحتيال. على كل موظف أن يعرف بمن يتصل وما يجب عليه فعله عند الاشتباه بنشاط احتيالي.

3-3-2-1 مسؤوليات الإدارة :

1-الإدارة هي المسئولة عن مكافحة الاحتيال. لذلك تتحمل الإدارة بشكل تام مسؤولية وضع وتحديد المسؤولية التنظيمية لمكافحة الاحتيال ومنعه.

2-تدل الدراسات الصادرة عن الشركات العالمية للاستشارات الإدارية أن سلوك كبار التنفيذيين في البنك، هو من أهم جوانب خلق مناخ أخلاقي في أي منشأة لذلك يجب أن يبدأ السلوك الصحيح من قمة الهرم وينتقل نزولاً إلى القاعدة عبر تصرّف كبار المسئولين بنزاهة وممارسة ما ينادون به ، ونظراً لأن سلوك الموظف ومواقفه داخل المنشأة المالية الكبرى تتأثر كثيراً بالإدارة العليا ، لذا يتعين على المدراء أن يكونوا القدوة بإتباعهم إجراءات الرقابة الصحيحة في أعمالهم اليومية وعدم خرق الإجراءات النظامية بحكم مواقعهم.

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-كما تدلّ الدراسات على أنه كلّما كان المدراء التنفيذيين على فهم وثيق بالعمليات المصرفية ، كلما انخفضت حوادث الاحتيال التي يتعرّض لها البنك.وبما أن سلوك الموظف ومواقفه داخل المنشأة المالية الكبرى يتأثر كثيراً بالإدارة العليا ، لذا يتعين على المدراء أن يكونوا القدوة بإتباعهم إجراءات الرقابة الصحيحة في أعمالهم اليومية وعدم خرق الإجراءات النظامية بحكم مواقعهم.

4-على المدراء أن يعوا مسؤولية الولاء لمركزهم في الكشف عن الاحتيال ومكافحته. ومن المهم توثيق مسؤوليات الإدارة عن كشف الاحتيال ومكافحته على مستوى استراتيجي في خطط الإدارة وكتيبات التشغيل.

5- على المستوى التشغيلي، تحدد مسؤولية الإدارة عن كشف الاحتيال ومكافحته في أوصاف الوظيفة وتعاميم وإجراءات المركز والفروع.

6- على المدراء أن يوفروا التوجيه اللازم والمساندة للموظفين حول الإبلاغ عن الاحتيال المشتبه به. فإذا بلّغ الموظفون عن ممارسات غير نزيهة ولم يتلقوا بعدها المساندة اللازمة من الإدارة تفقد سياسة الرقابة على الاحتيال مصداقيتها.

7-يتمتع المسئول عن مكافحة الاحتيال بمسؤوليات تمكنه من القيام بعمله على نطاق البنك. وليس من الضروري تولي هذه المهمة كوظيفة مستقلة بل يمكن تكليف أحد العاملين في البنك بالقيام بهذه المهمة إضافة إلى أعماله شريطة عدم التعارض بين المسؤوليات . لكن من الضروري أن يعطى الشخص المعين لهذه المهمة الصلاحية الكافية للتعامل مع الاحتيال بصورة فاعلة. ويجب في بعض الحالات أن يكون للمسئول عن الاحتيال حق الاتصال المباشر بالمستويات العليا للبنك .

3-3-2-2 لجنة مراقبة الاحتيال :

تلعب لجنة مراقبة الاحتيال لدى البنك دوراً رئيسياً في وضع السياسة والتثبت من أن السياسات والإجراءات والتدابير التي تتضمنها الإستراتيجية الشاملة لمراقبة الاحتيال يتم تطبيقها بصورة فعالة.

وتشرف اللجنة على تطوير عناصر الشروط الأساسية التسعة لمكافحة ومراقبة الاحتيال الواردة في هذه الدليل.

إنشاء لجنة لمكافحة الاحتيال لوضع السياسة وتنسيق ومتابعة تنفيذها وتقديم المساندة للرئيس التنفيذي ، على ألا تكون مهمة مكافحة ومراقبة الاحتيال محصورة بهذه اللجنة. بل يجب أن تشترك جميع مستويات الإدارة والموظفين بالطرق الصحيحة في تنسيق سياسة مكافحة ومراقبة الاحتيال ومتابعتها باستمرار والترويج لها.

تحدد سياسة مكافحة الاحتيال لدى البنك أعضاء اللجنة ومسؤولياتها.

تشمل اللجنة كبار المسئولين الذين يمثلون العمليات الرئيسية في البنك.

تجتمع اللجنة بشكل دوري ، وشهريا إذا أمكن، ولكن مرّة واحدة، على الأقل كل ثلاثة شهور. وأن يكون هنالك إمكانية عقد اجتماعات طارئة للبحث في حالات الاحتيال الخطيرة المشتبه بها.

5- من مهام اللجنة الرئيسية الإبلاغ عن الاحتيال ومساندة الرئيس التنفيذي بشأن جميع جوانب سياسة البنك لمكافحة الاحتيال.

3-3-2-3 وحدة التحقيق بشأن الاحتيال :

دور وحدة التحقيق بشأن الاحتيال هو تقصي حالات الاحتيال المحتملة ضد البنك. وتشمل هذه المسؤولية جمع وتقديم الأدلّة اللازمة لمساندة الإجراءات الإدارية أو التأديبية أو غيرها من الإجراءات والملاحقة القضائية و محاولة استرداد الأموال موضع الاحتيال.

إضافة إلى ممارسة مهمة التحقيق ، على وحدة التحقيق أن تقدّم ما يلي:

المساعدة والمعلومات والنصح إلى لجنة مراقبة الاحتيال.

المساعدة في تعزيز اكتشاف ومكافحة الاحتيال ونشر الوعي بشأنه.

المساعدة والتوجيه بشأن التدريب على مكافحة الاحتيال.

تقارير إلى قاعدة معلومات الاحتيال لدى مؤسسة النقد بصفة دورية حسب تعليماتها.

تقارير دورية للإدارة التنفيذية عن حالات الاحتيال

تقارير فنية بالتوصيات لسد الثغرات في أنظمة الرقابة الداخلية ، وأدلة السياسات والإجراءات .

إبلاغ ورفع مطالبات التعويض عن الخسائر الناتجة من حالات الاحتيال لشركات التأمين .

إنشاء قاعدة معلومات حول الاحتيال لاستخدامها من قبل وحدة مكافحة الاحتيال، لذلك قد تكون هذه الوحدة أصلح مجموعة في البنك للاحتفاظ بقاعدة المعلومات، وقد تقرر الإدارة التنفيذية أن تضع المسؤولية عن هذه المهمة في مكان آخر داخل البنك.

تشكل قاعدة المعلومات أداة هامة لكشف ومكافحة الاحتيال ولإدارة سياسة البنك لمراقبة الاحتيال. وينبغي، في سبيل المحاسبة وتسهيل المرجعية، أن تتضمن قاعدة المعلومات كل التفاصيل عن الاحتيال الفعلي والمشتبه به.

تشمل قاعدة معلومات الاحتيال، كحد أدنى، التفاصيل التالية عن كل حالة احتيال:

رقم مرجع (يرتبط بالسجلات المادية ذات الصلة).

الوضع الراهن ما إذا تم إقفال الملف أو مازال نشطاً.

المعلومات ذات الصلة والتواريخ أو الفترة التي جرى الاحتيال خلالها.

اسم أو أسماء المحتالين والأشخاص ذوي العلاقة سواء من موظفي

combat and control policy.

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

البنك أو من خارجه .
تقدير لقيمة الاحتيال المادية والأثر الشامل أو الأهمية الشاملة للاحتيال على عمليات البنك أو أدائه.
الموقع الجغرافي أو المادي للاحتيال.
طبيعة أو نقطة تركيز الاحتيال.
تحديد وسائل ارتكاب الاحتيال (أي الممارسات التي جرت).
الإجراءات التي تمت فيما يتعلق بالتحقيق.
نتائج الاستقصاء.
العمل التأديبي مثل التعويض و/أو الملاحقة القضائية التي جرت.
التدابير التي اتخذت لمكافحة الاحتيال.
تكون وحدة تقصي الاحتيال مسئولة عن تدريب المحققين وتأهيلهم .

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 المكافحة والاكتشاف :

التأكّد من وجود نظام فاعل لمراقبة الاحتيال يتصدى بحزم لمخاطر الاحتيال من حيث اكتشاف ومتابعة ومراقبة النشاطات الاحتيالية لاتخاذ الإجراءات اللازمة وبشكل عاجل بهدف التخفيف من خسائر الاحتيال المحتملة والحفاظ على السرية.
وضع إجراءات للتأكد من الملاحقة المستمرة أو تأديب الموظفين المتورطين بأعمال غير نزيهة.
تعزيز وتقوية السياسات والضوابط القائمة حيث تقتضي الحاجة.
تحديد وحدة مركزية تحول إليها جميع حالات الاحتيال المزعومة للموظفين وأفراد الجمهور.
مراجعة عملية استخدام الموظفين وغربلتهم واختيارهم بالنسبة لخطر الاحتيال.
التأكد من تطبيق إجراءات فاعلة بشأن الموظفين.
تحديد عملية استرداد أية خسائر حاصلة مثل تسوية المطالبات وتخفيف الخسائر والحد من الأضرار وعملية الاسترداد وإدارة مطالبات التأمين.
إبلاغ الإدارة عن حالات تضارب المصالح وانتهاكات سياسات البنك الجيدة وشكاوى العملاء.
تحديد عملية تسلسل رفع التقارير واتخاذ القرار بشأن حالات الاحتيال المشتبه به.
تقديم المشورة والتعديلات المطلوبة للرقابة الداخلية لمكافحة النشاط الاحتيالي.
وضع سياسات لحماية المتعاونين في الكشف عن الاحتيال.
مراجعة نتائج تقييم مخاطر الاحتيال.
التأكد من أن جميع مبادرات مراقبة الاحتيال تعطى الأولوية وتطبق

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

باستمرار.
وضع أنظمة لرفع التقارير إلى مؤسسة النقد .
المساعدة في تحكيم وتسوية الخلافات بين المجموعات الداخلية بشأن الأمانة وتشغيل مخصصات الخسائر.
المراجعة المستمرة لفعالية الإستراتيجية الشاملة والعناصر المختلفة لكل من الشروط الأساسية التسعة.

تحليل الاحتيال :
وضع قاعدة معلومات مصانة وموحدة لكافة حالات الاحتيال.
مراجعة الوضع الراهن لجميع حالات الاحتيال المبلغ عنها.
مراجعة حالات الاحتيال المبلغ عنها.
تحديد تفاصيل ونقاط ضعف الضوابط الداخلية والإجراءات والعمليات.
تحليل الاتجاهات وتحديد الأسباب وتقييم الحوادث بطريقة نظامية.

التوعية:
تحديد احتياجات وبرامج التدريب الصالحة لتوعية الموظفين بشأن الاحتيال.
الإشراف على برامج التثقيف والتوعية بشأن الاحتيال.
الإطلاع المستمر على تطورات وقضايا مراقبة الاحتيال بوجه عام وتوزيع معلومات الممارسات الأفضل عبر النشرات ووسائل الاتصال الأخرى حول الاحتيال في جميع أقسام البنك.

التحقيق بشأن الاحتيال :
تحديد سياسة كيفية معالجة الاحتيال وتقديم النصح والمساعدة للوحدات العاملة في التحقيق.
إجراء عمليات التقييم الأولية لجميع حالات الاحتيال المؤكدة.
المصادقة على الإجراءات التأديبية (مع أنه يمكن حدوث ذلك بطرق أخرى).
الإبلاغ:
التأكد من الإبلاغ عن جميع حالات الاحتيال في الوقت المناسب وباستمرار. وهذا يشمل كافة المعلومات مثل الفروع المحلية والخارجية والحوادث الداخلية والخارجية والاحتيال الفعلي والمحتمل أو المشتبه به.
تقديم التقارير الإحصائية إلى الإدارة.
رفع التقارير ومحاضر جلسات اللجنة إلى لجنة مراجعة إدارة المخاطر.
رفع التقارير إلى لجنة تدقيق الحسابات حول قضايا الاحتيال وتطبيق الاستراتيجيات الواردة في خطة مراقبة الاحتيال.

3-3-2-5 مسؤوليات الموظفين :
تقيداً بسياسة مراقبة الاحتيال لدى البنك، يتعين على الموظفين القيام

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:

بما يلي:

الإطلاع والتعريف بمفاهيمهم ومسؤوليات مراقبة الاحتيال ، مع أخذ تواقيعهم بالعلم .

اتخاذ قرارات مالية ونظامية وأخلاقية سليمة أثناء قيامهم بمهامهم ومسؤولياتهم اليومية.

قبول تحمل المسؤولية عن مراقبة الاحتيال في مجال عملهم ومسؤوليتهم.

3-4 الشرط الأساسي الثالث : تقييم مخاطر الاحتيال :

3-4-1 مقدمة :

يشكل الاحتيال جزءاً من الخطر التشغيلي. وفي سبيل التأكد من أن الإدارة تملك المعلومات اللازمة في محاولتها لمعالجة الاحتيال، يجب إجراء مراجعة هيكلية دورية لتقييم خطر الاحتيال تشمل جميع وظائف وعمليات البنك وتعالج هذه المراجعة أخطار الاحتيال الداخلي والخارجي على حد سواء، وأن تحدد مستوى وطبيعة انكشاف البنك لمخاطر الاحتيال. عندها تستطيع الإدارة أن تقرر التدابير المضادة التي تدعو الحاجة إليها . تخضع جميع المنتجات والخدمات الجديدة لعملية التقييم هذه إضافةً إلى مراجعة وتقييم المخاطر لكافة أدلة السياسات والإجراءات المتعلقة بتلك المنتجات والخدمات لمعرفة إذا ما قد تمّ تخفيف مخاطر الاحتيال. وحدها تلك العملية قادرة على تحديد وتقييم مخاطر الاحتيال وتبيان ما هي التدابير التي اتخذت و الإجراءات التي ما زالت هنالك حاجة لاتخاذها لتقليص وتخفيف هذه المخاطر.

3-4-2 الإرشادات :

إجراء مراجعة تقييم مخاطر الاحتيال دورياً بحيث تشمل جميع الوظائف ووحدات التشغيل في البنك على أن تعالج هذه المراجعة مخاطر الاحتيال الداخلية والخارجية على السواء لتحديد مستوى وطبيعة تعرض البنك لهذه المخاطر. ويسمح تحليل مخاطر الاحتيال بتطوير خطة لمراقبة الاحتيال توازي المخاطر المحددة.

قبل البدء، تخضع جميع المنتجات والخدمات المالية الجديدة لعملية تقييم المخاطر ويشمل ذلك معرفة ما إذا كان قد تمّ تخفيف هذه المخاطر وإمكانية إدارتها.

للتأكّد من الاحتفاظ بالصورة الحالية لتعرض البنك لمخاطر الاحتيال، من الملائم إجراء مراجعات دورية لتقييم المخاطر كل سنتين أو ثلاثة (أو أقل من ذلك إذا واجه البنك تغييرات هامة في محيطه).

توفر هذه المراجعة الدورية فرصة لإعادة تقييم جميع المخاطر المحددة في التقييم السابق، إضافة إلى توفير الفرصة لدمج المخاطر التي سبق تحديدها منذ المراجعة السابقة أثناء تقييم المخاطر للمنتجات الجديدة التي أدخلها البنك على عمله.

تمشيا مع الاتجاهات العالمية لجعل أعضاء مجلس الإدارة أكثر مسؤولية عن أعمال البنك، تتحمل الإدارة المسؤولية عن إجراء تقييم

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

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

لمخاطر الاحتيال. وقد يكون منتظراً من المراجع الداخلي والمراجع الخارجي أن يساهم مساهمة فعالة في ذلك أو أن يتأكد بأن عملية التقييم قد جرت فعلاً. تعتبر عملية التقييم أداة إدارية هامة، لا عملية محصورة في نطاق عمل تدقيق الحسابات.

3-4-2-1 عملية تقييم مخاطر الاحتيال :

تنطوي عملية تقييم مخاطر الاحتيال عادة على عدة مراحل كما يلي:

تحديد المجالات الوظيفية الرئيسية في البنك.

تقييم وتصنيف الطبيعة العامة لكل قطاع ومدى قابليته للاختراق.

التعرف على الأشكال المحددة لمخاطر الاحتيال في كل قطاع.

تقييم احتمال حدوث المخاطر المحددة في ضوء العوامل المعادلة مثل الضوابط الداخلية.

تقييم الأثر المحتمل على البنك من جراء حدوث المخاطر المحددة.

اقتراح وتطوير استراتيجيات للتخفيف من المخاطر المحددة أو التخلص منها كلياً.

يجوز أن تؤدي الاستراتيجيات المقترحة في المرحلة الأخيرة من عملية تقييم المخاطر الواردة أعلاه اتخاذ إجراءات لمكافحة الاحتيال أو إدخال إضافات أو تعديلات على إجراءات التشغيل أو الضوابط القائمة أو إدخال أنظمة وضوابط جديدة.

توجيه المسؤولية عن كل إستراتيجية للتقليل من المخاطر إلى فرد معين أو لجنة أو مجموعة معينة داخل البنك.

وضع جدول زمني مفصل لكل بند يحتاج إلى إجراء معين. وتوفر لجنة مراقبة الاحتيال في البنك الآلية المناسبة لمتابعة تنفيذ الإجراءات المحددة.

تسجيل عملية تقييم مخاطر الاحتيال وتوثيقها بشكل صحيح للإسناد مستقبلاً ولأغراض المحاسبة.

3-5 الشرط الأساسي الرابع : نشر الوعي بشأن الاحتيال وإفهام الموظفين أن الاحتيال حرام :

3-5-1 مقدمة :

على الإدارة أن تدرك بأن مساهمة الموظف في مكافحة الاحتيال هو أمر أساسي وأن أغلب حالات الاحتيال لن يتم اكتشافها أو مراقبتها بدون تعاون الموظفين. وفي سبيل زيادة وعي الموظفين وتعزيز التزام البنك بمكافحة الفساد، تدعو الحاجة إلى سلسلة من المبادرات المستمرة لوضع قضايا مكافحة الاحتيال واكتشافه والإبلاغ عنه أمام جميع الموظفين. و يكون التدريب على مراقبة ومكافحة الاحتيال عنصراً

إلزاميا من عناصر تدريب الموظف. وقد تدعو الحاجة إلى تطوير النشرات الإرشادية مثل كتيّبات عن أفضل الممارسات.
بالنسبة إلى الجمهور، هنالك حاجة لإطلاع العملاء ونشر الوعي بينهم بأن الاحتيال المرتكب ضد البنك هو أمر مرفوض وأن المرتكبين سيحالون إلى الجهات المختصة.

3-5-2 الإرشادات :

على الإدارة أن تدرك بأن مساهمة الموظف ، و موظفي الشركات المتعاقد معها في مكافحة الاحتيال هي أمر أساسي ، وأن أغلب حالات الاحتيال لن يتم اكتشافها أو مراقبتها بدون تعاون الموظفين.

3-5-2-1 وعي الموظف :

للفت انتباه جميع الموظفين إلى قضايا مكافحة الاحتيال ومراقبته والتبليغ عنه يقتضي وضع برنامج توعية متكامل.
قد تحتاج حلقات التدريب لنشر الوعي حول الاحتيال والأمن إلى مجموعة من العناصر والمضامين لتكون فاعلة. وتكون نقطة انطلاق التدريب رسالة تجعل كل موظف مسئولا عن المساهمة في مكافحة ومراقبة الاحتيال.
على حلقات النقاش ومواد التدريب أن تستعمل قدر الإمكان أمثلة واقعية وذات صلة مستخلصة من حالات فعلية في تاريخ البنك أو في بنوك أخرى.
يمكن لحلقات نشر الوعي ومجموعات النقاش أن تستخدم لمساندة حلقات التدريب الرسمي على أنظمة المراقبة والأمن. ويمكن أن تشمل المواضيع أموراً مثل سياسة البنك لمراقبة الاحتيال (لمحة عامة) والشئون الأخلاقية والحضارية ومسؤوليات الإدارة والموظفين وقواعد السلوك والإبلاغ عن الاحتيال.
يمكن استعمال الوسائل المرئية التعليمية في الحلقات والمقررات الدراسية أو العروض أو مجموعات النقاش. وتجدر الإشارة إلى أن مواد العرض المرئي المسبقة الإعداد هي أقل ثمناً من الوسائل المنتجة في البنك. غير أن بعض البنوك قد تجد بعض الصعوبة في العثور على عروض مرئية مسبقة الإعداد.
تلعب كتيبات الإرشاد حول السلوك الأفضل دوراً كخطوط إرشادية ومصادر مرجعيّة. أما أشكال الاتصالات المطبوعة الأخرى التي يمكن استعمالها لتعزيز رسالة مكافحة الاحتيال مرة تلو الأخرى بطرق مختلفة فهي تشمل الرسائل الإخبارية وبيانات الحقيقة والملصقات الإعلانية والمذكرات ويمكن الرجوع لإستراتيجية التحذير والتوعية التي تقوم بها مؤسسة النقد بالتعاون مع البنوك لمعرفة طرق ووسائل الإعلان والتوعية في سبيل مكافحة الاحتيال.
تطوير أنظمة لمتابعة وتقييم مصادر المعلومات حول السلوك الأفضل ولتوزيع المعلومات ذات الصلة، كما يمكن استخدام الانترنت لغرض

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 can not 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

توزيع المعلومات بصورة سريعة على أوسع نطاق داخل البنك.
الحاجة لتدريب خاص لمعالجة احتياجات المشتركين في الندوات المختارة. ويمكن الإقلال من اقتناص فرص الفساد والاستفادة غير الشرعية، التي غالباً ما ترتبط مع هذه الندوات إذا تمّ تدريب المشتركين على تحديد وتجنب السلوك غير السليم وتضارب المصالح. و الحصول من جميع المشاركين على تصريح بشأن انتفاء المصلحة (راجع الشرط الأساسي الخامس بعنوان "إجراءات الرقابة الداخلية للإطلاع على الإرشادات الخاصة بتجنب تضارب المصالح").
تعمل قواعد السلوك لدى البنك كإرشاد حول التوقعات الأخلاقية والمسؤوليات داخل البنك. لذلك فان قواعد السلوك تشكّل نقطة الانطلاق في الحملة لتعزيز مناخ العمل الأخلاقي والعنصر الأساسي فيه (راجع الشرط الأساسي التاسع بعنوان "معايير السلوك والتأديب" بهذا الشأن).

3-5-2-2 توعية العميل :

ثمة حاجة لتعزيز وعي الجمهور بأن الاحتيال المرتكب ضد البنوك وعملائها هو أمر مرفوض وان المرتكبين سيحالون إلى الجهات المختصة.
إشعار الجمهور من ناحية، أنه مسئول تجاه البنك وأن البنوك، من ناحية أخرى، مسئولة وتخضع للمساءلة عن الأموال الموجودة في حوزتها. لذلك فان الجمهور، على سبيل المثال، له الحق بأن يتوقع من البنوك اتخاذ كافة الإجراءات المعقولة والمناسبة لمراقبة الاحتيال.
يلعب العميل دوراً هاماً في المساعدة على مكافحة الاحتيال الخارجي والكشف عنه وفي مساندة هذا المسعى وتزويد المعلومات بشأنه من خلال التعاون في التبليغ فوراً في حال الاشتباه في عملية احتيالية.
تساعد التقارير السنوية والرسائل الإخبارية، على جعل العميل مطلعاً دوماً على الوضع. كما يمكن استخدام المعلومات الدورية والحملات الإعلانية لإطلاع الجمهور على أشكال الاحتيال التي تواجه البنوك وعلى أساليب اكتشافها.

3-5-2-3 توعية الأطراف ذات العلاقة :

على البنوك أن تعزز الفهم في أوساط الأطراف ذات العلاقة الذين يتعاقد البنك معهم بأن قواعد السلوك وسياسة مكافحة ومراقبة الاحتيال وغيرها من سياسات البنك ومعاييره المتصلة بالاحتيال والفساد هي أدوات لتعزيز العدالة والنزاهة والمحاسبة.
تضمين العقود التزاماً بالسلوك الأخلاقي والنزاهة. وكجزء من التقييم اللاحق للتعاقد يتم تقييم النتائج من حيث النوعية والنزاهة.

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.
A 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 enhance the understanding 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.

3-6 The Fifth Basic Condition: Internal Control Procedures

3-6-1 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.

3-6 الشرط الأساسي الخامس : إجراءات الرقابة الداخلية :

3-6-1 مقدمة :

الضوابط الداخلية هي العنصر الرئيسي في مكافحة الاحتيال. لذلك يجب وضع أنظمة رقابة داخلية موثّقة، في سياسة مكتوبة وبيانات إجراءات واضحة وشاملة لتقليص انتهاز فرص الاحتيال. كما يجب تكامل إستراتيجية المكافحة والمراقبة بالإجراءات التشغيلية والمستندات التي تحكم أنشطة جميع الإدارات ومرافق تسليم واستلام النقد والوظائف والموظفين.

والضوابط هي إجراءات تستخدم لخفض المخاطر إلى الحد الأدنى داخل العمل وهي مصممة لمنع الأخطاء واكتشافها وتصحيحها في الوقت المناسب عن طريق تطبيق التعليمات المتعلقة بما يلي:
- الموظفين
- الإجازات
- إحلال البدائل
- التدوير الوظيفي
- التدريب
- الموافقات والتعميدات
- الإثباتات .
- التسويات .
- مراجعة الأداء التشغيلي .
- أمن الأصول .
- فصل الواجبات .

يمكن تصنيف الضوابط على النحو التالي:
الضوابط الوقائية: لمنع وقوع الحوادث غير المرغوب فيها (مثل ضوابط الدخول الأمامية (Front-end access) مثل كلمات السرّ والأعداد التوافقية (Combinations) والإثباتات والحدود والحواجز الفعلية.
الضوابط الكشفية: لكشف وتصحيح الحوادث غير المرغوب فيها التي وقعت (أي الضوابط الخلفية (back-end controls) كالإثباتات والضوابط والأدلة والمراجعات والتسويات وآثار تدقيق الحسابات والتقارير.
الضوابط التوجيهية: لحثّ وتشجيع وقوع الأحداث المرغوب فيها (مثل السياسات والإجراءات وقواعد السلوك والكتيبات).
تتضمّن الضوابط الداخلية احتياطيات أساسية مثل فصل الواجبات. فالمسئولون عن الحراسة الفعلية للأصول يجب ألا يكونوا مسئولين أيضاً عن المساءلة بشأنها وعن التحقق من بيانات المحاسبة. تمكن تقنيات المراقبة الفاعلة البنك من :
اكتشاف الأخطاء عند وقوعها وتفادي الخسائر المكلفة.
حماية الموظفين النزيهين من نشاطات غير شريفة من قبل غيرهم من

الموظفين أو من عملاء البنك.
جمع الأدلّة اللازمة لتحديد الموظفين والعملاء غير النزيهين وملاحقتهم والقبض عليهم .

تطلب مؤسسة النقد من البنوك أن تضع موضع التنفيذ أنظمة رقابة داخلية كما ورد بالتفصيل في "إرشادات الرقابة الداخلية للبنوك التجارية". وتشكل هذه الأنظمة مجموعة شاملة من الإرشادات التي تحكم مختلف مجالات النشاط البنكي التجاري في المملكة. ومن الملائم قراءة هذا القسم من "مكافحة الاحتيال وإرشادات الرقابة" بالاقتران مع "إرشادات الرقابة الداخلية" وغيرها من التعاميم ذات الصلة وتعليمات العمل للحصول على لمحة عامة بشأن مطالب المؤسسة بشأن أنظمة الرقابة الداخلية للبنوك التجارية.
إن تطبيق هذه الإرشادات والإجراءات وتعليمات العمل هو أهم عنصر من عناصر الإستراتيجية الشاملة لكل بنك لإيجاد المناخ الذي يؤدي لمراقبة ومكافحة الاحتيال.
لا تشكل الإرشادات الواردة في هذا القسم قائمة شاملة ولا تحاول أن تغطي جميع المجالات التي تحكمها "إرشادات الرقابة الداخلية للبنوك التجارية". ولكنها ترمي إلى:
التأكيد على أهمية الضوابط الداخلية في مكافحة ومراقبة الاحتيال.
إبراز بعض المبادئ الرئيسية للرقابة الداخلية الناجعة.
توفير معلومات وإرشادات إضافية ترمي إلى تعزيز "إرشادات الرقابة الداخلية".

2-6-3 الإرشادات :

يوضع موضع التنفيذ أنظمة للرقابة الداخلية موثقة في سياسة مكتوبة وبيانات إجرائية واضحة وشاملة من أجل تقليص انتهاز فرص الاحتيال.
إجراء التكامل الوثيق بين إستراتيجية الرقابة الداخلية الشاملة والمستندات التشغيلية التي تحكم جميع الإدارات ومرافق تسليم واستلام النقد والوظائف والموظفين.
يتعين على البنوك أن تراجع "إرشادات الرقابة الداخلية للبنوك التجارية" للبحث عن أمثلة عن إرشادات الرقابة الداخلية والأساليب والإجراءات. وعلى البنوك، بالإضافة إلى ذلك، أن تستنير بإرشادات وتعاميم المؤسسة وجميع الأنظمة والتعليمات المصرفية المطبقة في المملكة، وذلك للحصول على فهم شامل ومفصل عن الشروط الرسمية الخاصة بالضوابط الداخلية.
الإرشادات التالية ترمي إلى تعزيز المعلومات بشأن إجراءات الرقابة الداخلية الواردة في المستندات المشار إليها.

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.

3-6-2-1 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.

3-6-2-1 المبادئ الرئيسية للرقابة الداخلية الفاعلة:

تحكم الضوابط الداخلية المكتوبة الفعالة ما يلي:

الوصول المقيَّد والمراقب إلى مناطق الخطر.

صيانة وأمن الموجودات القيّمة بشكل فعلي، بما في ذلك المرافق والموجودات والسجلات والملكية الأدبية.

التعميد الصالح ومستويات الصلاحيات لجميع الموظفين.

الفصل الناجح بين المسئوليات ، خاصة في المجالات المالية والمحاسبة وتسليم واستلام النقد أو الأوراق المالية.

تسجيل جميع الصفقات والحوادث والاشتباهات ونتائج التحقيقات.

نتائج التحقيقات غير العادية أو غير المتوقعة.

أساليب الإبلاغ.

المساءلة عن النتائج على كافة المستويات.

بعد تطبيق أنظمة الرقابة يتم متابعتها باستمرار ومراجعتها بانتظام لاختبار فعاليتها. فعلى سبيل المثال انهيار بنك "بيرنغز" وهو من أقدم بنوك بريطانيا التجارية عام 1995، يذكرنا بنتائج قصور الرقابة الداخلية . فالتحقيق الرسمي في الحادث أثبت أن انهيار البنك كان نتيجة نشاطات غير سليمة لم تكن معتمدة وغير صحيحة التوقيت قام بها شخص واحد لم يتمّ اكتشافه في الوقت المناسب نتيجة قصور الإدارة والضوابط الداخلية التي تعد من الأساسيات في العمل المصرفي.

المبررات الشاملة لعدم التقيد بالضوابط هي أنها لم تعد منطقية أو أن الوقت الكافي لم يكن متوفراً أو أنها غير صالحة. من المهم إبلاغ هذه الملاحظات إلى الإدارة لتقييم الحاجة إلى تقييم الضوابط.

خلال فترات التغييرات التنظيمية الهامة، يزداد خطر المساءلة لأجزاء من العمل والغموض بشأن مسؤوليات الإبلاغ. يجدر بالإدارة العليا في هذه الظروف أن تؤكد على وضوح خطوط المسؤولية وعلى المتابعة المستقلة للضوابط الداخلية عند كل مرحلة من مراحل التحوّل.

3-6-2-2 ممارسات التوظيف :

تبيّن الإحصائيات أن خطر الاحتيال الأكبر الذي يواجه البنك يأتي من موظفيه لوحدهم أو بتعاونهم مع أشخاص من الخارج.

التذكير أن بوسع الموظفين على اختلاف مستوياتهم الوظيفية أن يلزموا حالياً نسبة كبيرة من موجودات البنك وموجودات عملائه عن طريق نشاطاتهم التجارية. وهذا مما يعطي النزاهة الأساسية لجميع الموظفين المزيد من الأهمية.

تعتبر نزاهة الموظف شرط مسبق لنجاح أي نظام رقابي. فاختبار

النزاهة قبل التعاقد مع الموظف يجب أن يتمّ لضمان الحصول على موظفين جديرين بالثقة والاعتماد عليهم. فعلى المدراء ، إضافة إلى استمارة طلب التوظيف التفصيلية والاستناد إلى عدة مراجع، أن يتدربوا على مهارات المقابلة للتأكد من تحديد سلوك غير شريف في تاريخ الموظف وتقييم احتمال حدوث مثل هذا السلوك في المستقبل. ويتعين على البنك أن يدون المراجع التي يسميها الموظف المرشح ويقارنها مع مراجع مستقلة. و التحقق من المؤهلات العلمية والمهنية. من الأهمية قبل التعاقد مع موظف جديد التأكد من أن هذا الموظف لم يسبق له أن اشترك في حالات احتيال أو اختلاس في منشأة مالية داخل أو خارج المملكة من خلال مراجعة المعلومات المقدمة من الموظف الجديد والتأكد من صحتها ومخاطبة المعرفين واتخاذ كافه الإجراءات اللازمة للحد من تعيين موظفين لهم سلوك احتيالي سابق.

التأكد قبل التعاقد مع الموظفين الجدد إذا ما كان يعمل في وظيفة أخرى وينوي الاستمرار فيها، أو إذا ما كان يمارس نشاط تجاري وذلك تحقيقا لمبدأ الحماية من تضارب المصالح ، وينطبق هذا الإجراء على موظفي الشركات المتعاقد معها.

من الضروري مراجعة السلوك النزيه دون توقف. هنالك الآن قوائم واسعة من "الأعلام الحمراء" المتوفرة لمساعدة المدراء على فرز الأفراد المحتمل ارتكابهم لأعمال احتيالية. وتشمل هذه الأعلام الحمراء غالباً مزايا سلوكية واجتماعية مثل:

الإثراء غير المبرّر والتبدّل المفاجئ في أسلوب العيش.

الموظف الذي يعمل دوماً بعد ساعات العمل الرسمية.

فقدان المستندات الأصلية واستبدالها بصور عنها.

الاستعمال المفرط لسوائل التصحيح.

التردد في أخذ الإجازة.

رفض الترقية.

استقالة الموظف الجديد بسرعة.

إصرار بعض الموردين أو المقاولين أو العملاء على التعامل مع موظف معين.

العلاقات الحميمة مع الموردين أو المقاولين أو العملاء التي تنقطع فجأة.

مراقبة الموظفين القدامى الذين أحرزوا معرفة واسعة بإجراءات الأمن في البنك، خاصة حيث تقع نزاعات متصلة بالعمل أو حيث يزيد عدد الموظفين عن الحاجة.

تزويد الموظفين بمستندات مكتوبة واضحة مثل وصف الوظيفة والسياسات والإجراءات وتعليمات العمل التي تحدد كل جانب من جوانب مهماتهم وواجباتهم.

إلمام الموظف بكامل حقوقه وواجباته في جميع الأمور المتعلّقة

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.

An employee who always works after the official work hours.

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

بالاحتيال.

تشمل أساليب المتابعة والرقابة ما يلي:

اتفاقيات السرية.

الإجازات الإلزامية.

تبديل برامج الموظف ومهام عمله على فترات غير متوقعة.

تدقيق حسابات الموظف الذي يذهب في إجازة.

لا يجوز أن يسمح للموظفين من ذوي القرابة أن يعملوا معاً، لا سيما في المجالات المالية والمحاسبة وتسليم واستلام النقد أو الأوراق المالية.

و العمل على أخذ مجموعة من الصور الفوتوغرافية للموظف للمساعدة في حال اختفائه أو في حال كان ضحية لمحاولة ابتزاز.

يجب أن يولي البنك كل اعتبار لمضامين امتناع الموظفين السابقين عن إعطاء مراجع صريحة. ويجب صرف المرتكبين الثابتين من الخدمة دون مرجع وملاحقتهم.

3-6-2-3 فصل الواجبات :

تطبيق مبدأ فصل الوظائف والواجبات بكل صرامة في جميع المجالات والأنشطة التشغيلية حيث ينطبق ذلك. يتطلّب هذا المبدأ أساساً فصل الذين يؤدون واجبات تشغيلية عن أولئك الذين ينفذون الضوابط ويتولون مهمة الرقابة. كذلك الأمر فصل الرقابة على الموجودات عن رقابة المستندات المتعلقة بهذه الموجودات.

تم تجميع الأمثلة التالية من مختلف مجالات العمل لإيضاح مبدأ فصل الواجبات.

1. فصل وظائف استلام الضمانات والإفراج عنها إلى المقترضين عن تدوين القيود في سجل الضمانات.

2. فصل تحصيل الدين عن وظيفة تحديده.

3. فصل مهمة جدول الرواتب عن مهام إدارة الموظفين.

4. فصل عمليات المتاجرة في المكتب الأمامي والمكتب الخلفي. فمع أن المطلوب من المتعاملين، مثلاً، أن يراقبوا تقيدهم بالحدود، لا بد وأن يخضعوا للرقابة المستقلة الشديدة من المكتب الخلفي أو الوسطي.

5. فصل وظائف طلب شراء المواد القابلة للاستهلاك والمعدات وبنود التخزين عن وظيفة استلام السجلات والاحتفاظ بها وتعميد الدفع.

فتضمن "إرشادات الرقابة الداخلية للبنوك التجارية" إشارات عدة لحالات تتطلب فصل الواجبات بشكل فعّال.

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

.

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.

3-6-2-4 الرقابة المزدوجة :

حيث تخضع أساليب الأمن (مثل المفاتيح ومبادئ وأساليب الإنذار وأمن أماكن النقد) لتقنيات الرقابة المزدوجة بكل شدة. وتجدر في هذه الشأن ملاحظة ما يلي على سبيل المثال:

للإقلال من فرص الاستحصال دون تفويض على نسخ المفاتيح، لا يجوز للموظفين بأي حال من الأحوال المشاركة في مفاتيح تعود لمجموعة الحراسة المزدوجة. وينطبق ذلك على الإعداد التوافقيـــة (Combinations) للخزنة الموضوعة تحت الحراسة المزدوجة.

ألا تحتوي صناديق المفاتيح على مجموعة من مفاتيح "الطوارئ" بشكل نسخ غير معتمدة من المفاتيح الموضوعة تحت الحراسة المزدوجة.

الإبلاغ فوراً عن المفتاح المفقود ودون استثناء. وينطبق هذا حتى في الحالات التي تتوفر فيها نسخ للمفاتيح.

إذا كان للموظف سبب للشك بأن سريّة أحد الأعداد التوافقية الموضوعة تحت الحراسة المزدوجة قد خرقت عليه الإبلاغ عن ذلك فوراً.

وضع إجراءات لاسترداد المفاتيح وأساليب الدخول الأخرى بشكل دوري كما يتم وضع إجراءات للتأكد من تبديل المفاتيح وكلمات السر وأدوات الحراسة المزدوجة الأخرى بشكل دوري .

حضور موظف الرقابة دوماً في مناطق النقد المعينة ، ومكائن الصرف الآلي .

حيث أن المحتالين غالباً ما يستعملون الفترة التالية مباشرة لعملية التصحيح لارتكاب الاختلاس، يجب إجراء عمليتي تصحيح كامل لمرفق مناولة النقد عند اكتشاف خلل كبير في ميزان احتساب النقد.

تجري عملية التصحيح الأولى عند اكتشاف الخلل وتجرى الثانية بعد تحديد سبب الخلل.

3-6-2-5 سياسة قبول الهدايا :

حيث أن الموظف معرّض للرشوة عن طريق الهدايا أو لصرف انتباهه عن الصفقات ، يجب وضع سياسة مكتوبة تمنع ذلك وكيفية تضمين ذلك في سياسة البنك لمكافحة الاحتيال ، وفي كتيب الموظف الذي يعده البنك يجب أن تمنع هذه السياسة بشكل عام الموظف من الأمور التالية:

قبول أية هدايا أو إغراءات أو ضيافة مقابل تقديم خدمة نظامية أو غير نظامية.

إعطاء معلومات رسمية حصرية أو سرية مقابل أي إغراء.

سوء استخدام وظيفته السابقة والحالية للحصول على أسعار تفاضلية للصفقات الخاصة.

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.

3-6-2-6 الحسابات الراكدة :

أن تكون مراقبة الحسابات الراكدة سياسة مستمرة . راجع "إرشادات الرقابة الداخلية" وتعاميم المؤسسة ذات الصلة للإطلاع على الإرشادات الخاصة بالحسابات الراكدة.

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.

3-6-2-7 مناولة النقد (تسليم واستلام) :

هنالك عدد من حالات التعرّض للمخاطر في مجال تسليم واستلام النقد تحكمها مجموعة من الإجراءات (راجع "إرشادات الرقابة الداخلية" بهذا الشأن) ، يخضع تطبيقها الصحيح لحملات مفاجئة لتدقيق حسابات النقد بصورة منتظمة في الأماكن المخصصة وأمانة الصناديق. ويشمل الانكشاف لمخاطر النقد النشاطات المتصلة بما يلي:

مراقبة وإدارة النقد في أمانة الصناديق.

نقل النقد من الأماكن المخصصة إلى الصندوق.

الوصول إلى خزانة أمين الصندوق وإلى النقد عندما لا يكون أمين الصندوق على رأس عمله أو بعيداً عن الصندوق حتى ولو لفترة قصيرة.

الحالة الفعلية وأمن الأقفال والخزائن.

للتأكّد من حسن المساءلة عن النقد، أن تكون قواعد مناولة النقد لأمناء الصناديق في فروع البنك والموظفين الآخرين العاملين في مجال مناولة النقد واضحة ومتماسكة.

تطبق الإرشادات المتعلقة بأختام أمين الصندوق وأدوات التعليم الأخرى واستمارات التعميد والمفاتيح وقواعد الدخول ومجموعة الأعداد التوافقية، ومتابعتها وتقييمها بصورة منتظمة لاستمرار فعاليتها.

إغلاق الأماكن المخصصة لأمناء الصندوق وتحديد الأشخاص المصرح لهم بالدخول إلى تلك المناطق.

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.

3-6-2-8 حدود السحب :

تحديد حدود السحب المكشوف والكمية والصفقة، حسب الانطباق لأمناء الصناديق والمتاجرين والمسئولين وغيرهم من الموظفين الذين يتعاملون بالنقد وبالإدارات المالية غير النقدية أو المستندات القابلة للتداول.

أن تعكس هذه الحدود المخاطر المحتملة ومستوى الخطر الذي بمقدور الإدارة تحمله.

متابعة هذه الحدود بدقة وتنفيذها بشدّة.

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.

3-6-2-9 الإشراف على غرفة المتاجرة :

الفصل الواضح للواجبات في غرفة أو غرف المتاجرة لدى البنك من الأمور الأساسية لأي نظام رقابة فعال.

تشمل عبارة "المكتب الخلفي" عادةً قيود حركة الاتجار والتسويات والتصحيحات. وفي غالب الأمر وبحكم الضرورة يعمل موظفو المكتب الخلفي بصورة وثيقة مع الذين يتولون أعمال البيع والشراء

على أساس يومي. ولكن لا يجوز السماح بتطوير هذه العلاقة الوثيقة في العمل بحيث يصبح المكتب الخلفي خاضعاً للمتاجرين.

يتولى الإشراف على نشاطات الاتجار فريق مستقل من مهامه إدارة المخاطر كجزء من إشراف هذه الإدارة المستمر على جميع أنواع المخاطر. وتكون مهمة هذا الفريق التفتيش المستقل للتأكّد من أن المتاجرين يعملون ضمن حدودهم وأن أي تجاوز لهذه الحدود يتم الإبلاغ عنه والحصول على تعميد به على وجه السرعة وأن الحساسية لتقلبات السوق وأثرها على قيمة المركز المالي تم تقييمها والإبلاغ عنها. كما يتأكد فريق التفتيش من إعادة احتساب الأرباح والخسائر بشكل منتظم وأن تتم تسوية ذلك في السجلات المحاسبية وإذا اقتضى الأمر السجلات التي يحتفظ بها المتاجرون.

أن يكون لدى البنوك إجراءات موثّقة وضوابط تغطي جميع أوجه تقديم الصفقة وحساباتها والإبلاغ عنها. وعلى الموظفين الذين يطلب منهم الانحراف عن هذه الإجراءات والضوابط أن يسألوا عن السبب وإذا لم يقتنعوا بالجواب ينبغي تشجيعهم على رفع الأمر فوراً إلى الإدارة العليا.

على المراجع الداخلي أن يخضع نشاطات غرفة المتاجرة إلى التدقيق الشديد والمنتظم.

على الإدارة أن تنظر بحذر إلى الحالات التي يبدو فيها أن فرداً واحداً بإمكانه الإجابة على كل الأسئلة الرئيسية حول نشاط معين أو منتج معين.

من الأمور الضرورية إيجاد خطوط إبلاغ واضحة واتصالات فعّالة بين كبار المسئولين خاصة في حال تولي الفروع عمليات المتاجرة في مناطق جغرافية متباعدة أو فيما وراء البحار .

حيث يكون للبنوك عمليات دولية ، من الأهمية عدم الإخلال بنزاهة الضوابط الخاصة بنشاطات المكاتب الخارجية. وعلى المدراء المسئولين القيام بزيارات متكررة بالحد المعقول إلى المكاتب الخارجية التي تتولى أعمال المتاجرة للبنك، خاصة عندما يكون المكتب على بعد جغرافي من المكتب الرئيسي ، وأن تشمل هذه الزيارات التباحث مع المتاجرين ومدراء الأخطار ومدراء المكتب وموظفي المساندة حول النشاطات والتحدث مع المنافسين لنشاطات المكتب والمتاجرين فيه.

ولا تستطيع الإدارة أن تتأكّد من استلامها المعلومات الصحيحة وطرحها الأسئلة الصحيحة وقدرتها على ترجمة إشارات التحذير بشكل صحيح إلا إذا كان لديها الفهم الكافي للعمل والإحساس به.

قد لا تتعاطى الإدارة المحلية للفروع الخارجية بالقرارات اليومية لهذه الفروع ولكن يجب أن يكون لها سلطة التصرف للتأكد من تقيد هذه الفروع بمعايير الرقابة التي يضعها البنك (بالزيارات المفاجئة مثلاً

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 mangers, 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

لتلك الفروع).

هنالك خطر كبير من عدم إيجاد مكان طبيعي للأنشطة الخارجة عن المألوف (مثل بعض المشتقات المالية والمنتجات المعقدة) في هيكلية البنوك مما يضعف مستوى الإدارة والإشراف. لذلك يجب إخضاع هذه النشاطات إلى مستوى عالي من الرقابة الإدارية.

المبدأ الرئيسي للإدارة الحكيمة هو الحفاظ على أنظمة متشدّدة بشأن التثبّت والتصحيح في مهمات التسوية بصرف النظر عما إذا كانت الدفعات ستذهب لشركات المجموعة أو لأطراف ثالثة.

visits to these branches).

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 إدارة تضارب المصالح :

على البنوك أن تضع وتنفّذ سياسات وإجراءات لمنع حدوث تضارب المصالح وحل التضاربات التي تقع. ويجب توثيق هذه الإجراءات في كتيب الموظف وفي الإرشادات الأخرى ذات الصلة. ويجب أن تشمل قواعد السلوك السياسة الخاصة بتضارب المصالح أو أن تشير إليها.

يحق للعملاء والمؤسسات الخارجية والمقاولين ومقدمي طلبات التوظيف وموظفي البنك أنفسهم أن ينتظروا من البنك القيام بواجباته بطريقة منصفة وغير منحازة وألا تتأثّر سياسة البنك بالمصلحة الذاتية أو الربح الشخصي.

ينشأ تضارب المصالح عندما يقع موظفو البنك، أو يبدو أنهم وقعوا تحت تأثير المصالح الشخصية أثناء عملهم. وقد يكون الإدراك الحسي بتضارب المصالح مضراً بقدر ما هو عليه التضارب الفعلي لأنه يهزّ الثقة في نزاهة البنك المعني وموظفيه.

قد ينطوي تضارب المصالح على كسب مالي قد ينتج، على سبيل المثال، عن موظف، أو فرد من أفراد عائلته يملك عقاراً أو حصصاً أو مركزاً في شركة تتقدم بعطاء للحصول على عقد مع البنك، ويتلقى في الوقت نفسه هدايا أو ضيافة أو دخلاً من وظيفة ثانية. وليس من الضروري أن يكون هنالك ثمن نقدي لأن تضارب المصالح قد يتمثل باختيار مقدم عطاء معين للحصول على عقد أو تعيين أحد الأقرباء أو الأصدقاء في مركز معين.

تحديد مجالات تضارب المصالح المحتمل كجزء من تقييم خطر الاحتيال. وتشمل أعمال البنك حيث يمكن حدوث تضارب مصلحة فيها ما يلي:

مجال العطاءات والمشتريات .

تعيين الموظفين .

العمل بدون أجر والتوظيف الثانوي (متدربين) .

الهدايا والمنافع والضيافة .

الموافقة على القروض وغيرها من أشكال الاعتمادات .

التعامل بالأوراق المالية.

على كبار المسئولين في البنك، أو على أي مدير، أو أي موظف آخر

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

من العاملين في هيئات الاستقدام أو لجنة اختيار العروض، أو كعضو في أية مجموعة داخلية أخرى تتعاطى بالاختيار، أو الموافقة أو وضع السياسة أو اتخاذ القرارات أن يعلنوا خطياً للبنك عن أية مصالح لهم تتصل بعملهم وقد تؤثر في قدرتهم على الاشتراك في تقييم القضايا المطروحة بصورة حيادية. و استخدام سجل مصالح نموذجي لهذا الغرض.

المصالح التي يتوجب اعتبارها "ذات صلة وهامة" هي:

عضوية مجالس الإدارة، بما فيها الأعضاء غير التنفيذيين الذين يحتلون مناصب في شركات خاصة (باستثناء الشركات الراكدة).

الملكية الكاملة أو الجزئية لحصص في شركات خاصة وأعمال ومؤسسات استشارية من المحتمل أن تسعى للتعامل مع البنك.

امتلاك حصص في مؤسسات من المحتمل أن تسعى للتعامل مع البنك (باستثناء امتلاك الحصص في وحدات صناديق الائتمان أو الترتيبات المشابهة حيث لا يكون للعضو أي تأثير على الإدارة المالية).

أية علاقة مع أية مؤسسة تتعاقد لتقديم خدمات للبنك أو للانتفاع بخدمات البنك.

على أعضاء مجلس الإدارة أن يصرحوا عن مصالحهم ذات الصلة في اجتماعات المجلس، أو في الاجتماعات المرتبطة بالمجلس، أو في الاجتماعات الخاصة بالموافقة على عطاء واختيار الموظفين أو أي عطاء تنافسي آخر وأن يتم التصريح شفهيا في بداية الاجتماع ويجب تسجيل هذا التصريح في محضر الاجتماع. وإذا وقع التضارب في المصلحة خلال الاجتماع على العضو المعني أن ينسحب من الاجتماع وألا يلعب أي دور في المناقشة أو التصويت على القرار المعني.

تؤدي بعض جوانب إجراءات الاختيار والموافقة إلى نشوء تضارب في المصالح يمكن أن يعطي أحد المنافسين الأفضلية على منافس آخر في إرساء العقود. وللتخفيف من هذا الاحتمال يتم اتخاذ الخطوات التالية :

1- ألا يتمّ إعداد مواصفات الخدمات المطلوبة بطريقة من شأنها أن تعطي الأفضلية لمورد معين. لذلك يتوجب في حال الحاجة لاستشاريين لإعداد المواصفات، أن يكون ثمة إجراء تقييم لعلاقاتهم التجارية مع الموردين المشتركين في العطاء.

2- لا يجوز إعداد إجراءات تقييم عطاءات الموردين المتنافسين بطريقة تعطي الأفضلية لمورد معين. وهذا الأمر يشير ضمناً إلى التصريح من جانب المشتركين في اختيار مقدمي العطاء عن أية مصلحة مالية أو صلة اجتماعية أو قربى مع الموردين المحتملين.

3- يجب أن يوضع موضع التنفيذ إجراءات للتخفيف من النشاط غير النزيه بين الموظفين المشتركين في عملية اتخاذ القرار والموردين. وهذا يشمل ترتيبات تفرض على الموردين المحتملين التصريح عن أية علاقة تجارية أو اجتماعية حميمة أو علاقة قربى لهم مع أي موظف

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:

Membership of the boards of directors, including non-executive members who hold positions in private companies (excluding inactive companies).

Full or partial ownership of shares in private companies and consultative businesses and firms that might seek to deal with the bank.

Ownership of shares in firms which may seek to deal with the bank. (with the exception of owing shares in the units of investment funds, or similar arrangements in which the member has no influence on the financial administration).

Any relation with any firm that enters into a contract to offer services for the bank or to benefit from the bank's services.

Members of the board shall disclose their relevant interests at the board's meetings, at the meetings for approving a bid, or the meetings for approving appointment of employees or any other competitive bids. The disclosure must be stated verbally 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

في البنك يشارك في اختيار أحد المنافسين.
4- حيث يعمل المتاجرون كمدراء علاقات مع العملاء في الوقت الذي يتولون فيه مسؤولية الاتجار لحساب البنك الخاص، لا بد أن تنشأ مخاطر محتملة مثل سوء توزيع الصفقات وإخفاء معاملات الحسابات الشخصية. وللتخفيف من هذه المخاطر على الإدارة أن تمارس فصلاً دقيقاً ومتشدداً للضوابط.

3-6-2-11 حماية الملكية الفكرية:

يجب أن يشمل تعريف البنك "للأمن المادي" حماية البنك وبيانات عملائه إلى جانب الملكيات الفكرية الأخرى مثل برامج الكومبيوتر التي يطورها البنك داخلياً.
يجب حماية الأماكن التي تخزَّن فيها هذه البيانات من أي مخاطر داخلية أو خارجية ويجب أن يقتصر حق الوصول إلى هذه البيانات على من يحتاج إليها وأن يضبط الوصول إليها عن طريق أنظمة دخول بالمفاتيح والبطاقات والأرقام السرية.
يتعين على كل موظف أو مؤسسة تعمل لصالح البنك أو نيابة عنه أن يعبئ ويوقع على تعهد نظامي للمحافظة على السرية وأن يحدد هذا التعهد بالتفصيل المسؤوليات المتعلقة بعدم الكشف عن هذه المعلومات بطريقة غير صالحة أو غير مناسبة، وتعرَّف المعلومات السرية بأنها المعلومات غير المتوفرة للجمهور العام التي يملكها البنك ويمكن للفرد ذو العلاقة أو للبنك الوصول إليها.
يقتضي تخزين البيانات والسياسات الاحتياطية التأكد من تطبيق ترتيبات أمن البيانات على نسخ الأقراص الاحتياطية وغيرها من الوسائط المادية المخزنة في مواقع نائية.
يجب تمزيق أوراق القمامة أو التخلص منها بطريقة مماثلة وإتلاف الوسائط الأخرى مثل ديسكات البيانات بطريقة آمنة.
يجب إتباع سياسة مكتبية واضحة للحفاظ على السرية. ويجب تصميم هذه السياسة بحيث تضمن قيام الموظفين بنقل جميع المعلومات السرية والمحصورة التوزيع أو الحساسة عند غيابهم عن المكتب لأي فترة طويلة من الوقت، لا سيما في نهاية كل يوم عمل، ويجب نقل هذه المواد عن مكتب الموظف وتخزينها في منطقة آمنة مخصصة لكل فرد ولكل مكتب.
على البنك أن يراجع بانتظام إجراءات وسياسات الرقابة الداخلية وتحديثها ليتمكن من التعامل مع المخاطر الجديدة المتصلة بالاختلاس أو بالمعلومات المملوكة.

3-6-2-12 أمن أنظمة المعلومات :

اكتشاف نشاط الإرهاب الالكتروني ("Cyber Terrorists") يشكل عنصراً هاماً في حماية شبكة المعلومات وأنظمتها. ولكن معظم الاعتداءات على شبكات البنوك تأتي من داخل البنك ويرتكبها أشخاص من الداخل مثل الموظفين الحاليين والموظفين غير المعتمدين

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

والأطراف الأخرى ذات العلاقة الذي يعرفون كيف يلحقون الأذى بالبنك بصورة محددة وقاسية وسريعة.

على البنك أن يضمن سياسة مكافحة ومراقبة الاحتيال وأن تتضمن إشارة إلى سياسة أو قاعدة سلوك لاستعمال الحاسب الآلي. ويجب أن تحدد مثل هذه السياسة الأمنية معايير استعمال معدات الحاسب الآلي لدى البنك ويجب أن تتضمن إرشادات وضوابط حول استعمال شبكة الانترنت الخاصة بالبنك والبريد الالكتروني وحق الدخول إلى شبكة الانترنت.

على مدراء الشبكة أن يكونوا سباقين في تقييم نقاط الضعف في الشبكة وتحديد أفضل المواقع لتطبيق تدابير الأمن وتسليط الأضواء على النشاط المحظور.

يجب استخدام أدوات صالحة لإدارة الأمن لضمان نزاهة وسرية وتيسر الشبكة. وتعني كلمة "نزاهة" في هذا السياق أن تكون المعلومات دقيقة ومحمية ضد التعديل العرضي أو المتعمد. وتعني كلمة "السرية" أن المعلومات لا تصل إلا إلى المفوضين بالإطلاع عليها. وتتيح الأدوات الإدارية التقنية للمدراء القدرة على الإدارة المركزية لتوقيع المستعمل على السياسات الأمنية وتطبيقها واكتشاف خروقات الأمن السارية المفعول ومتابعتها وفحص النظام لتحديد مدى قابليته للاختراق وإنتاج التقارير الشاملة حول الاستخدام العادي للشبكة، إلى جانب محاولات إساءة استعمال الموظفين لما لهم من امتيازات.

تحتاج جميع التعديلات التي تطرأ على أنظمة المعالجة إلى الاعتماد والتوثيق والمتابعة.

13-2-6-3 الدعوات الاحتيالية :

قد يجد البنك نفسه أمام دعوة لأن يلعب دوراً ما في صفقة احتيالية في حقيقتها، ويتم عادة طرح مثل هذه الدعوة كصفقة معقدة ذات قيمة مالية عالية توفّر فرصاً جذابة لتمويل منخفض الكلفة أو استثمار ذي مردود كبير. وتنطوي هذه الدعوات عادةً على أدوات مالية (مثل شهادات الإيداع أو سندات أو ضمانات مصرفية ممتازة) تحمل اسم مؤسسة مالية غير معروفة أو نائية جغرافيا. والمثال المعروف هو ما يرتكبه عدد من النقابات الاحتيالية الدولية المعروفة باسم " Advance Free Fraud / Telefax scam"

تشكّل هذه الدعوات مخاطر مالية مباشرة ومخاطر تشويه سمعة البنك. وقد يكون الغرض النهائي للمحتالين هو الحصول على دفعة ما (مثل الرسم المسبق). ولكن هدفهم من مقاربة البنك قد يكون الحصول على مستندات تضيف المصداقية والاحترام لأساليبهم. وحتى الخطاب الذي لا يتضمن عرض عمل قد يوفر الوصول إلى صلب أوراق البنك أو توقيع أحد أعضاء مجلس إدارته.

إذا عرض على البنك أي عمل هام دون أن يكون عن طريق عميل قديم وموثوق به أو عن طريق شريك مالي، على البنك أن يمارس

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 mangers 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 who is, not an old and trustworthy customer or a

أقصى درجات الحذر للتثبّت من طبيعة ومصادر الصفقة والموصي بها.

فيما يلي الأوصاف التي قد تحذر البنك من طبيعة الصفقة الاحتيالية:

بلد المنشأ: على البنك اخذ الحيطة والحذر اعتماداً على بلد المنشأ .

تثبيت العزم على المشاركة: غالباً ما يطلب المحركون للعملية في مرحلة مبكرة توثيقاً كتابياً للرغبة والقدرة على الدخول في الصفقة. وستستعمل أية مستندات مرسلة من هذا النوع لارتكاب الاحتيال.

نسب عوائد غير واقعية: من أجل حث المستثمرين أو المقترضين وغيرهم من المساهمين في الصفقة، يعرض أصحاب المشروع عوائد مرتفعة غير واقعية وكلفة اقتراض متدنية كحافز للاشتراك. ويمكن أن تكون قيمة الصفقة ضخمة.

- **السرية وشروط الغرامة:**

تشترط الدعوة بأن تبقى طبيعة الصفقة و/أو أطرافها طي الكتمان لأسباب تنافسية ولا يجوز الكشف عنها إلا بعد توقيع جميع الأطراف على الاتفاقية أو بعد دفع الرسوم المحددة. وقد تحمل شروط السرية غرامات في حال عدم الالتزام.

- **التعقيد :**

غالباً ما تكون الصفقة بالغة التعقيد دون أي سبب ظاهر في بعض الحالات. ومن المحتمل أن يبالغ أصحاب المشروع باستخدام مصطلحات غير مفهومة لتكوين انطباع بالخبرة العميقة.

– استخدام الفاكس والانترنت – ترسل معظم المستندات، إن لم يكن كلّها، المتبادلة بين الأطراف عن طريق الفاكس أو الانترنت مما يسهّل تزوير الأحرف وإخفاء مكان إقامة الوسطاء والمحتالين.

– أتعاب الأطراف الأخرى: حيث ينطوي المشروع على الأموال يطلب غالبا إجراء دفعات لطرف ثالث لا علاقة له بالمشروع.

3-7 الشرط الأساسي السادس : عملية المتابعة :

3-7-1 مقدمة :

على الإدارة أن تتأكّد من وجود عملية متابعة مستقلة وموثوقة. وأن تحظى المتابعة الداخلية ونشاطات الرقابة على مساندة منتظمة من مقيِّمين خارجيين مستقلين مثل مدققي الحسابات الخارجية.

3-7-2 الإرشادات :

على الإدارة أن تتأكّد من وجود عملية متابعة مستقلة وموثوق بها. المتابعة الداخلية المستمرة والأنشطة الرقابية هي عادة من مهمات مدقق الحسابات الداخلي وإدارة المخاطر أو إدارة سلامة النوعية أو

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.

الرقابة الداخلية.
مساندة المتابعة الداخلية بتقييم مستقل منتظم يجريه مقيِّمون خارجيون مثل مراجعو الحسابات الخارجيون. وعلى الإدارة أن تتصرف بسرعة بشأن تقارير مراجعو الحسابات الخارجيين لإصلاح نقاط الضعف في الرقابة ومتابعتها والتأكد من تطبيقها.
متابعة فاعلية سياسة مكافحة ومراقبة الاحتيال من قبل لجنة مراقبة الاحتيال.

3-7-2-1 المتابعة الداخلية:

تبدأ متابعة الضوابط الداخلية بقيام الإدارة التنفيذية والمدراء والمشرفون بنشاطاتهم اليومية في مجالات الإشراف والفحص والرقابة والتوجيه (أو باستخدام مشروع التقييم الذاتي للمخاطر وإجراءات الرقابة (CRSA) ،
قد يعتمد مجلس الإدارة على الخبراء في الإدارة لتسيير أعمال البنك اليومية، ولكنه يبقى المسئول الأول والأخير عن متابعة أعمال البنك. ويمكن لمجلس الإدارة أن يتابع أعمال البنك من خلال التقارير الإدارية ولكن عليه أن يفعل أكثر من استلام هذه التقارير ومراجعتها. عليه أن يكون متأكداً من دقتها وموثوقيتها. لذلك يجب أن تكون التقارير الإدارية الداخلية التي يعدها البنك صالحة لاتخاذ القرارات الإدارية التي تستند عليها الإدارة والسماح لها بعد ذلك بمتابعة نتائج هذه القرارات.
أن يكون أعضاء مجلس الإدارة وكبار الإداريين على قناعة تامة بأن أنظمة إدارة المخاطر والرقابة الداخلية لديهم تعمل بشكل صحيح. وتقع على الإدارة التنفيذية المسؤولية الأساسية في توفير هذه القناعة. وقد يقرر مجلس الإدارة الاستعانة برأي حيادي مستقل عن رأي الإدارة التنفيذية ، وتوفر مهمة تدقيق الحسابات الداخلية مصدراً هاماً في هذا الشأن من داخل البنك، إذ أنها تتولى مهمة تطبيق برنامج رقابة مستمرة تراجع وتختبر فيما إذا كانت إجراءات التشغيل الصادرة عن المجلس تخضع لضوابط كافية تعمل بشكل صحيح وتتقيد مع سياسات المجلس والأنظمة.
يوفر تدقيق الحسابات الداخلي نقطة التركيز المستمر على الضوابط الداخلية والمراقبة الدورية لجميع جوانب أعمال البنك. وعلى مدقق الحسابات الداخلي أن يراجع تقيد البنك بالسياسات المعتمدة والأنظمة المرعية . ومع أن البنك هو الذي عليه أن يقرر عدد المرات التي يحتاجها مدقق الحسابات الداخلي لمراجعة عمليات محددة فإن المجالات التي تصلح لمزيد من التدقيق تشمل المجالات التي تشكل أكبر حجم من المخاطر الكامنة (مثل مخاطر الاحتيال في هذه الحال) أو تلك التي أظهرت ضعفاً في المراجعات السابقة.
كلما زاد حجم العمل التجاري أو مخاطره أو تعقيداته أو انتشاره الجغرافي كلما زادت الحاجة لمدققي حسابات داخليين من ذوي الخبرة

يتمتعون بقدرات فنية ومهارات في قطاعات السوق ذات الصلة.
على مدقق الحسابات الداخلي أن ينسق نشاطاته مع المراجعين الخارجيين ويزودهم بالمعلومات الأساسية، و أن يتمتع رئيس التدقيق الداخلي بحق الاتصال المباشر بالرئيس التنفيذي ، ورئيس مجلس الإدارة، ورئيس لجنة تدقيق الحسابات بصرف النظر عن الشخص الذي تقدم له التقارير.
إحدى مسؤوليات لجنة تدقيق حسابات البنك هو الإقناع التام بفاعلية مهام التدقيق الداخلي.
عند إعداد تقارير التدقيق الداخلي يجب إبراز نقاط الضعف الرئيسية في الرقابة ويجب عندها الاتفاق على خطة عمل إدارية لمعالجة الضعف ووضع جدول زمني لذلك. وتقع على الإدارة مسئولية تطبيق توصيات التدقيق الداخلي وأن تتأكد عند ظهور قضايا كثيرة من إجراء المعالجة بطريقة سليمة وفي حال ظهور نقاط ضعف يجب أن يخطط المدقق الداخلي لزيارات لاحقة ضمن فترة وجيزة من إنهاء التدقيق للتأكد من أن التدابير التصحيحية قد تم اتخاذها . فإذا تخلفت الإدارة عن تنفيذ توصيات المدقق الداخلي يجب إبلاغ لجنة تدقيق الحسابات بذلك.
تجدر الإشارة بأن مدققي الحسابات الداخليين لا يمنعون الاحتيال بصورة آلية ، فهم يعملون أولاً كمراقبين مهمتهم التأكد من أن معايير المحاسبة تطبق وأن الإجراءات الإدارية تنفذ بشكل صحيح وأن البنك يتقيد بالأنظمة المحلية . لهذا السبب يجب تعيين دور تطوير خطط العمل والإجراءات التشغيلية لمعالجة الاحتيال المحتمل إلى إدارة المخاطر أو وحدات التدقيق التشغيلي أو إلى وحدات مماثلة. ويعتبر عدد من المؤسسات هذا الدور كجزء من مهمة إدارة المخاطر الشاملة يساندها ويساعدها التدقيق الداخلي وغيره من الأدوات المعنية في تطوير الاستراتيجيات لمعالجة المشاكل المتعلقة تحديداً بالاحتيال.
نقترح أن ينشأ البنك وظيفة مستقلّة لإدارة المخاطر تشرف على جميع نشاطات العمل التجاري وتغطي جميع جوانب الخطر. وتكون الأغراض الرئيسية لهذه الوظيفة هي تحديد وتحليل وتقييم ومتابعة المخاطر المتّصلة بأية مهمة أو إجراء داخل البنك للتأكد من أن نشاطات البنك تسير وفقا لسياسات مجلس الإدارة بالنسبة لمخاطر السوق والمخاطر التشغيلية والائتمانية. وفي هذا الشأن تساهم إدارة المخاطر مساهمة رئيسية في تطوير الضوابط الداخلية والاحتفاظ بها ومتابعتها.
فيما يتعلّق بتدابير مراقبة ومكافحة الاحتيال ، أهمية تعيين مهام محددة للتدقيق الداخلي وإدارة المخاطر وضمان النوعية والرقابة الداخلية وغيرها من الإدارات المعنية. وتكون هذه المهام إضافة إلى أو جزء من نشاطات المتابعة التي تمارسها هذه الإدارات من خلال عملها اليومي.
تُنشأ البنوك وحدة خاصة للالتزام (compliance) يرأسها لجنة أو

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 workas 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

مسؤول التزام. ويراجع برنامج الالتزام عادةً سلسلة واسعة من الضوابط مثل حدود الإقراض النظامية والضرائب وقضايا الأوراق المالية وشروط تقديم التقارير والكشف. وقد ينتظر من مسئول الالتزام(Compliance Officer)، فيما يعود لمكافحة ومراقبة الاحتيال، أن يصدر التوجيهات بشأن أثر القوانين والأنظمة الجديدة بالنسبة للاحتيال على أعمال وإجراءات البنك وأن يقيّم التقيد بهذه الأنظمة والتعليمات وتوجيهات مؤسسة النقد .

لا تتعاطى لجنة مراقبة الاحتيال عادة ومباشرة متابعة الرقابة الداخلية. ويقتصر عملها في هذا الشأن على جمع المعلومات ذات الصلة حول جهود المتابعة التي يبذلها البنك لأغراض الإبلاغ المستمر عن سياسة مكافحة ومراقبة الاحتيال.

control and internal control and other concerned departments. These tasks shall be in addition to, or part of the follow-up activities carried out by these departments during their daily work.

Banks should establish a special unit for compliance headed by a committee or a compliance officer. The compliance program usually reviews a wide range of controls, such as the regular lending limits, tax and securities issues, reporting requirements and disclosure. With regard to combat and control of fraud, the compliance officer is expected to issue guidance on the impact of new regulations and laws on fraud regarding the bank business and procedures; and to assess compliance with these laws, regulations and directives of SAMA.

The fraud control committee shall not usually be involved directly in the follow-up of internal control. Its work in this connection shall be limited to the collection of relevant information on the follow-up efforts made by the bank for ongoing reporting on the policy for combating and controlling fraud.

3-7-2-2 External Follow-up

The bank shall undertake the responsibility of evaluating the effectiveness of the bank's internal controls, and the bank's internal and external auditing bodies shall be entrusted with the implementation of the bank's responsibility. SAMA will also assess the effectiveness of the systems of internal controls at the bank as part of its examination program.

Evaluation by external evaluators is essential to provide an independent and neutral confirmation of the effectiveness of the internal operational controls, validity of management systems, accounting controls and correctness of financial information. The external auditor also provides an assessment with regard to the quality, reliability and strategy of internal auditing function at the bank. The board of directors should be aware of the performance of internal auditors.

The effectiveness of the external auditing in the detection and combat of fraud must not be overestimated. External auditors focus on submission of financial reports to determine the extent of compliance with accounting standards and regulations and laws in force. As far as the risk of fraud results from the failure of such compliance, the work of external auditors provides a certain level of control of fraud. However, non-compliance of this type, which the external auditors are used to reveal in the assessment, does not constitute an adequate instrument for revealing risk of fraud in banking. Consequently, fraud must be confronted primarily through operating and control systems, as well as through the internal and external auditing,

3-7-2-2 المتابعة الخارجية :

تقع على عاتق البنك مسؤولية تقييم فعالية ضوابط البنك الداخلية وتتولى مكاتب تدقيق الحسابات الداخلية والخارجية في البنك تنفيذ هذه المسؤولية. كما تقوم مؤسسة النقد بتقييم فاعلية أنظمة الضوابط الداخلية لدى البنك كجزء من برنامج فحص البنك من قبل المؤسسة.

التقييم على يد مقيّمين خارجيين هو أمر أساسي لتوفير تأكيد مستقل ومجرّد لفاعلية الضوابط التشغيلية الداخلية وصلاح الأنظمة الإدارية وضوابط المحاسبة وصحة المعلومات المالية. كما يزود المدقق الخارجي فيما يتعلّق بنوعية وإستراتيجية مهمة التدقيق الداخلي لدى البنك ومجلس الإدارة يجب أن يكون على علم حول أداء مدققي الحسابات الداخليين.

عدم المبالغة بفعالية التدقيق الخارجي في اكتشاف الاحتيال ومكافحته. فمراجعو الحسابات الخارجيين يركزون على تقديم التقارير المالية والأنظمة الإدارية لتقرير مدى التقيد بالمعايير المحاسبية والأنظمة المتبعة. وبقدر ما ينتج خطر الاحتيال جراء التقصير في مثل هذا التقيد فإن عمل المدققين الخارجيين يوفر مستوى معين من ضبط الاحتيال. ولكن الإجراءات التي اعتاد المدققون الخارجيون استخدامها في التقييم لا تشكل مصادر إضافية في مخاطر الاحتيال المتعلقة بالأعمال المصرفية. لذلك يجب مجابهة الاحتيال بصورة رئيسية عن طريق أنظمة التشغيل والرقابة يضيف إليها التدقيق الداخلي والخارجي عنصراً آخر من عناصر التدقيق.

يمكن أن يؤدي استخدام المدققين الخارجيين كاستشاريين للإدارة إلى

تضارب في المصلحة عندما يتولى المدقق الخارجي للحسابات مسؤولية وضع النظام المحاسبي ويطلب منه في فترة لاحقة تقييم هذا النظام عند إجراء عملية التدقيق الخارجي. لذلك يتعين على البنوك أن يوازنوا بين موضوع تضارب المصلحة المحتملة وكلفة استخدام مراجع خارجي للقيام بعمليات مترابطة وما يوفر ذلك من وقت. والمعايير المهنية السائدة تسمح للمدقق بتدقيق حسابات خارجية من خلال القيام بعملية خارجة عن التدقيق لعميل واحد شريطة ألا تتأثّر بذلك موضوعية المدقق واستقلاليته، وعلى البنوك التي ترغب في استخدام المراجعين الخارجيين لخدمات استشارية أخرى أن تحاول الفصل بين الاستشارة التي يمكن للمدقق أن يقدمها والمسؤولية الإدارية أو التنفيذ التشغيلي التي لا يجوز أن يتولاها مراجع الحسابات.

3-7-2-3 سياسة متابعة مراقبة الاحتيال ومكافحته :

تتولى لجنة مراقبة الاحتيال متابعة تنفيذ سياسة مراقبة ومكافحة الاحتيال، و إبلاغ نتائج هذه المتابعة إلى الإدارة العليا ومجلس الإدارة.

تشكل الإجراءات التالية أمثلة على المؤشرات الإحصائية الرئيسية (إضافة إلى أية إجراءات أخرى يحددها أي بنك معين) التي يمكن استخدامها لمتابعة فاعلية سياسة البنك لمراقبة الاحتيال.

مدى الاختلاف بين المخاطر التي يقيّمها البنك والتي تقيّمها هيئات الضمان.

مدى الاختلاف بين قيمة فعالية الضوابط التي يقيّمها البنك وتلك التي تقيّمها هيئات الضمان.

عدد حالات الاحتيال العادية المشتبه بها وعدد مثل هذه الحالات التي لم تبرز أثناء تقييم الاحتيال.

عدد حالات الاحتيال الكبير المشتبه بها وعدد مثل هذه الحالات التي لم تبرز أثناء تقييم الاحتيال.

عدد أيام العمل بين البدء بمعالجة الاحتيال والانتهاء منه.

النسبة المئوية بين عدد وقيمة حوادث الاحتيال الثابت وعدد وقيمة حالات الاحتيال المزعوم المحالة للتحقيق.

عدد قيمة الاستردادات بالنسبة إلى عدد وقيمة حالات الاحتيال المزعوم المحالة للتحقيق.

على لجنة مراقبة الاحتيال أن تزود الإدارة التنفيذية بتقارير منتظمة حول العمليات الإحصائية الواردة أعلاه و تحديث هذه المعلومات كل ربع سنة على الأقل.

على التدقيق الداخلي أن يتولى مراجعة حسن تنفيذ سياسة مراقبة ومكافحة الاحتيال كل سنتين على الأقل، أو بعد أية تغييرات هامة في

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:

Extent of the difference between the risks assessed by the bank and risks assessed by insurance bodies.

The difference between the effectiveness of controls evaluated by the bank and those evaluated by insurance bodies.

Number of cases of normal suspected fraud and the number of such cases that have not arisen during the assessment of fraud.

Number of big suspected fraud cases and the number of such cases that have not arisen during the assessment of fraud.

Number of working days from the beginning of addressing fraud cases to the time when the addressing has ended.

The difference between Percentage of 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.

مجالات عمل البنك. ويجب استعمال نتائج هذه المراجعة لإعادة تطوير سياسة مراقبة ومكافحة الاحتيال بما يحسن الأداء ويعزز السياسات والإجراءات.أن يتبع هذه المراجعة إعادة تقييم لواقع خطر الاحتيال في البنك. ولا يكون ذلك ممكنا إلا إذا اشتركت جميع وحدات وإدارات البنك في عملية تقييم المخاطر ومراقبة واقع المخاطر على أساس مستمر، لا سيما عند حدوث تغييرات هامة في مجالات العمل أو في مخاطر العمل أو في الضوابط.

3-8 الشرط الأساسي السابع : أنظمة الإبلاغ عن الاحتيال :

3-8-1 مقدمة :

وضع نظام رسمي للإبلاغ الداخلي عن الاحتيال الفعلي والمشتبه به موضع التنفيذ. وإبلاغ جميع الموظفين بوضوح بهيكلية هذا النظام وإجراءات التعامل مع الإبلاغ عن النشاط الاحتيالي. وكجزء من هذا النظام ، وضع السياسات والآليات المناسبة لحماية المشتبه بهم (لو لم تثبت ضدهم أي أنشطة احتيالية) نتيجة الإبلاغ عن النشاطات الاحتيالية. و تطوير آليات لتسهيل وتشجيع العملاء أو الجمهور على الإبلاغ عن حالات الاحتيال المشتبه به داخلياً وخارجياً. و تطبيق سياسة رسمية بشأن الإبلاغ الخارجي إلى جهات مثل مؤسسة النقد والجهات الأمنية المختصة.

3-8-2 الإرشادات :

وضع نظام رسمي للإبلاغ الداخلي عن الاحتيال الفعلي أو المشتبه به موضع التنفيذ، و إبلاغ جميع الموظفين بوضوح بهيكلية هذا النظام وإجراءات التعامل مع الإبلاغ عن النشاط الاحتيالي.

تتأثر الترتيبات المطلوبة بحجم البنك وهيكليته (مثل عدد الفروع ومواقعها وعدد الوحدات التشغيلية).

يغطي التدريب الأولي هيكليات وإجراءات الإبلاغ الموصوفة أيضاً في كتيب الموظف وفي سياسة مكافحة ومراقبة الاحتيال.

يجب إعداد خلاصة دقيقة مركزة عن ترتيبات الإبلاغ عن الاحتيال توزع على جميع الموظفين وتنشر بانتظام على لوحات الإعلان وفي الرسائل الإخبارية الداخلية.

من أجل ضمان السلوك السليم الصالح للمشتكين في متابعة شكواهم و تدريب الموظفين على ما يلي:

كيف يجب أن يتصرفوا في حال مشاهدة سلوكاً غير سليم في موقع العمل.

ما هي آليات الإبلاغ الداخلي المتاحة وكيف تعمل هذه الآليات.

ما هي الإجراءات الوقائية لحماية الذين يستخدمون آليات الإبلاغ.

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.

ما هي قنوات الإبلاغ الخارجي المتاحة.
تشجيع الموظفين على تقديم الشكاوى مع عدم إغفال الاسم. ولهذه الغاية من المهم أن يكون لدى الموظف قناعة صحيحة بأن الأمر سيعامل بسرية وان هناك آليات وجدت لحمايته ضد أي عملية انتقام.
أهمية أن يدرك الموظف بأن الاحتيال المشتبه به يجب أن يبلغ عنه. ذلك أن محاولة الاحتيال الفاشلة هي بخطورة المحاولة التي تؤدي إلى خسارة فعلية للأموال ما لم يتم الإبلاغ عنها فإنها ستوفر للمرتكب فرصة الاستفادة من التجربة للمحاولة مرة أخرى.
إبلاغ المشتكين أن شكواهم أخذت بعين الاعتبار وأن التدابير المناسبة ستتخذ، و إبلاغ المشتكين بالنتيجة النهائية في كل الحالات.
أن يتم وضع برنامج للتحفيز للموظفين الذين يقومون بالتبليغ عن حالات الاحتيال حال اكتشافها .

3-8-2-1 قنوات الإبلاغ :

ترفع شكاوى الموظفين وتقاريرهم، بوجه عام، إلى رئيس الموظف المباشر ومن الأفضل تقديم خلاصة مكتوبة عن الشكوى. وعلى الرئيس، بدوره أن يرفع الأمر مباشرة إلى أحد أفراد الإدارة العليا المعني.
في حال كان الرئيس هو المعني بالشكوى، أو إذا كان لدى الموظف أية مخاوف مبررة من رفع التقرير إلى رئيسه المباشر أن يكون هنالك قناة بديلة لرفع تقرير سري مباشرة إلى عضو الإدارة العليا المعني.
إذا كان التقرير ضد عضو الإدارة العليا، يجب أن تكون هنالك قناة إبلاغ إلى الرئيس التنفيذي في البنك.
التفكير بإنشاء خط هاتفي ساخن (hot line) يمكن للموظف استخدامه للإبلاغ عن الاحتيال الفعلي والمشتبه به، و دمج هذا الخط مع قنوات الإبلاغ الأخرى والإجراءات الواردة في هذا القسم.
من المنتظر من الموظفين، بوجه عام ، أن يتبعوا قنوات الإبلاغ داخل البنك. ولكن يجب إشعار الموظفين بجواز الإبلاغ عن أي سلوك فاسد مباشرة إلى مؤسسة النقد ، إذا لم يكن الموظف راغبا في إبلاغ الأمر إلى رئيسه المباشر أو إلى عضو الإدارة العليا المعني أو إلى الرئيس التنفيذي .

3-8-2-2 حماية البلاغ :

كجزء من نظام الإبلاغ عن الاحتيال، ينبغي تطوير آليات وسياسات

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

مناسبة لمساندة المشتكين وحمايتهم من عمليات الانتقام نتيجة الإبلاغ عن نشاطات احتيالية.
أن يوضح كتيب الموظف وسياسة البنك لمراقبة الاحتيال ومكافحته بأن عقوبات قاسية ، تشمل الاتهام بسوء السلوك والملاحقة النظامية وإنهاء الخدمة، تتخذ بحق الشخص الذي يقوم بالتعدي على أي شخص يبلغ عن الاحتيال أو الفساد.
لا يحظى المبلغ بالحماية إذا تبين بالتحقيق أن الشكوى رفعت بطريقة كيدية أو عن سوء نية.
اتخاذ إجراءات محددة لإزالة المخاوف من عملية الانتقام والشعور السائد بين الموظفين بأن المبلِّغ عن الاحتيال والفساد قد يلحق به الأذى. ويجب إيصال هذه الرسالة إلى جميع الموظفين بصورة واضحة ومنتظمة عبر الرسائل الإخبارية وغيرها من وسائل الاتصالات الداخلية.

3-8-2-3 الإبلاغ الخارجي :
يحتاج كل بنك لوضع سياسة رسمية واضحة وإجراءات تفصيلية للإبلاغ عن النشاط الاحتيالي والفساد إلى مؤسسة النقد و السلطات الأمنية المختصة.
الاحتيال هو عمل إجرامي. وعندما يعتقد البنك بعد إجراء التحقيق أن ثبوت عملية الاحتيال يتوجب إحالة الأمر إلى الشرطة وإبلاغ المؤسسة بذلك. يمكن كذلك أن تكون شركات أخرى، كشركات التأمين، معنية بالأمر في حالات معينة ويجب تحديدها كجزء من سياسة البنك الشاملة.
لا تقلل مطالبة البنك بالإبلاغ عن الاحتيال من صلاحيته في تقرير المعالجة المناسبة الواجب تطبيقها مثل الملاحقة القضائية أو الإجراء الإداري أو العلاج المدني أو استرداد المال عن طريق إجراءات تأديبية أو التوقف عن اتخاذ أي إجراء آخر.
يلعب تدخل الشرطة، لا سيما عندما يكون المبلغ المعني كبيراً، دوراً هاما في تخفيف الخسارة والضرر الناتج عن الاحتيال. وقد تكون الشرطة، باستخدام مواردها الذاتية أو بالتعاون مع الانتربول أو أية هيئة دولية أخرى تعمل في مجال تنفيذ النظام، قادرة على اعتراض أو تجميد الأموال المسلوبة أو على الحيلولة دون إتلاف الدليل. لذلك من المهم أن تسمح سياسة مكافحة الاحتيال لدى البنك من اتخاذ قرار سريع على مستوى الإدارة التنفيذية في سبيل تطبيق إجراءات الحد من الضرر وحماية مصالح البنك دون تأخير في حالات الاحتيال والفساد الخطيرة.
على البنك أن يشعر المؤسسة بجميع حالات الاحتيال المصرفية ، والاحتيال المشتبه به.
لا يقلل إبلاغ المؤسسة من مسؤولية البنك عن إحالة قضايا الاحتيال

إلى الشرطة أو الجهات الأمنية الأخرى ذات الاختصاص مثل وحدة التحريات المالية (F I U) عند الحاجة .

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.

3-8-2-4 استلام التقارير من العملاء والجمهور :

تطوير آليات لتسهيل وتشجيع قيام العملاء والجمهور بالإبلاغ عن حالات الاحتيال المشتبه بها والاحتيال الخارجي. وعلى البنوك، مثلا، أن تفكر بالطريقة المثلى لاستلام الشكاوى والتقارير المتعلقة بالاحتيال من العملاء والمواطنين العاديين لمعالجة هذه الشكاوى والتقارير. ويمكن للبنوك أن تستخدم صفحاتها على الشبكة العنكبوتية لهذا الغرض.

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 الشرط الأساسي الثامن: معايير التحقيق :

3-9-1 مقدمة :

تزويد موظفي التشغيل وموظفي التحقيق الداخلي بإرشادات وإجراءات رسمية واضحة للتأكد من معالجة واستقصاء الاحتيال بكفاءة متى تمّ اكتشافه. و أن تكون أدوار وواجبات جهاز التحقيق محددة بوضوح ومفهومة. يجب أن تضمن المعايير التي يضعها البنك موضع التنفيذ إجراء التحقيقات بسرعة وفعالية بحيث يمكن في كل حالة احتيال مشتبه بها اتخاذ القرار المناسب بالشكل السريع . و وضع هيكلية لمعلومات وتوثيق الرقابة تضمن حماية الأدلّة والاحتفاظ الملائم بالسجلات. و أن يكون في متناول الإدارة هيكلية إبلاغ لمتابعة التحقيقات كما يجب إبلاغ مؤسسة النقد بجميع حالات الاحتيال الكبيرة.

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 الإرشادات :

تزويد موظفي التشغيل وموظفي التحقيق الداخلي بإرشادات وإجراءات رسمية واضحة للتأكد من معالجة واستقصاء الاحتيال بكفاءة متى ما تم اكتشافه. وتحمل إجراءات معالجة الاحتيال والتحقيق بشأنه أهمية خاصة في المراحل الأولى بحيث لا تمس بالتحقيقات اللاحقة.

تدريب الموظفين قد يكون مطلوبا وربما شمل ذلك التدريب الخاص لموظفين مختارين.

الاحتفاظ بسجل لجميع حالات الاحتيال المكشوف عنه والتحقيقات التي أجريت، و وضع أنظمة لمتابعة التحقيق والإبلاغ عن وضعه ونتائجه وتحديثه بشكل مستمر. وعلى الإدارة أن تستخدم التقارير لمتابعة التحقيقات ومن المفروض أن تستلم الإدارة العليا أو لجنة مراقبة الاحتيال تقارير منتظمة ومبرمجة حول وضع وسير التحقيقات.

دور الإدارة هو دور توجيهي ولا يجوز لها أن تتعاطى مباشرة في عملية التحقيق أو أن تتدخل فيها.

directly get involved or intervene in the process of the investigation.

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):

The date and time of the notification, incident or suspicion.
The name of the complaint (if applicable).
The name of the notifier, the incident or suspicion.
The details of communications.
The nature of the notification.
The time or period of alleged fraud.
The circumstances of the alleged crime.
The location of the alleged crime
The name or names of the accused.
The address (es) of the accused.
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.

3-9-2-1 استلام بلاغ باحتيال مزعوم :

استخدام هيكليات مسؤولية مناسبة (راجع الشرط الأساسي الثاني بعنوان "الإطار التنظيمي وهيكليات المسؤولية") وقنوات الإبلاغ (راجع الشرط الأساسي السابع بعنوان "أنظمة الإبلاغ عن الاحتيال").

أن يتم إيضاح مسؤوليات الشخص الذي يتلقى بلاغا عن احتيال مشتبه به أو مكشوف عنه في إجراء مشمول في إرشادات مراقبة ومكافحة الاحتيال لدى البنك.

المسؤولية الرئيسية لمستلم مثل هذا البلاغ أو للشخص الذي يكتشف احتيالا أو فساداً محتملاً هي أن يسجل جميع تفاصيل البلاغ أو الاشتباه بأسرع وقت ممكن في ملف سري يشار إليه كتقرير قضية.

تشمل التفاصيل المتوجب تسجيلها ما يلي (بدون أي ترتيب أو أولوية معينة):

تاريخ ووقت البلاغ أو الحادث أو الاشتباه .
اسم المشتكي (إذا كان الأمر منطبقاً) .
اسم المبلغ أو الحادث أو الاشتباه.
تفاصيل الاتصالات.
طبيعة البلاغ.
وقت أو فترة الاحتيال المزعوم.
ظروف الجريمة المزعومة.
موقع الجريمة المزعومة.
اسم المتهم أو أسماء المتهمين.
عنوان أو عناوين المتهم أو المتهمين.
مبلغ الاحتيال المزعوم.
أي بلاغ كتابي يتم استلامه يجب تأريخه وختمه ومعالجته بنفس الطريقة التي يعالج به البلاغ الشفهي بالاحتيال.

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.

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.

3-9-2-2 التقييم الأولي :

غرض التقييم الأولي لاحتيال مشتبه به هو تقرير ما إذا كان ثمّة ما يشكل أساسا للبلاغ أو الاشتباه وأفضل الوسائل المتوجب اتخاذها.

التدقيق السريع في جميع حالات الاحتيال المزعوم ولا يجوز إنذار المرتكب المشتبه به بالتقييم الأولي.

تجدر الإشارة إلى أن المتهم له حقوق بموجب النظام. ولا يجوز اتخاذ أي إجراء (مثل استجواب الموظفين) دون التشاور المسبق مع الإدارة العليا ولجنة مراقبة الاحتيال، ومسئول مراقبة الاحتيال وغيرهم من الموظفين حسب الانطباق، كما ورد في نظام الإبلاغ عن الاحتيال لدى البنك.

قد يؤدي عدم إتباع الإجراءات القائمة فيما يخص تقصي الاحتيال

واستجواب الموظفين المتورطين إلى إفساد العمل التأديبي ويعطل نجاح أية ملاحقة في المستقبل.
حماية سرية المشتكي والمستلم للبلاغ.
إجراء التقييم الأولي بعد أن يكون الموظفون المدربون تدريباً مناسباً قد جمعوا أية معلومات استدلالية متوفرة لهم شرط ألا يعطل جمع هذه المعلومات أي تحقيق لاحق.
استناداً إلى المعلومات المتوفرة، اتخاذ القرار اللازم بشأن الإجراء الواجب اتخاذه والذي يشمل التوصل إلى واحد من الاستنتاجات التالية:
أن لا أساس للشكوى ولا لزوم لأي إجراء لاحق.
أن القضية يجب أن تحال إلى مدير أعلى أو إلى وحدة التحقيق في أعمال الاحتيال لدى البنك للمزيد من التحقيق.
أن القضية تحتاج إلى مشورة من المؤسسة أو من الشرطة أو من أية هيئة قانونية معنية أخرى بشأن ارتكاب أو عدم ارتكاب الجرم.
تسجيل القرار في تقرير القضية إلى جانب ما يلي:
سبب القرار
المادة النظامية التي استعملت كأساس للقرار
الإجراءات الواجب اتخاذها (إذا وجدت)
هوية الشخص أو السلطة الخارجية المسئولة عن اتخاذ أي إجراء لاحق
اسم و مركز الشخص الذي اتخذ القرار
تاريخ القرار
الخيارات المحتملة لتولي التحقيق تشمل الشرطة ومراجعي الحسابات الخارجيين والمحققين الخارجيين وموظفي البنك الداخليين مثل وحدة أو مدير مكافحة الاحتيال أو مدققي الحسابات الداخليين أو وحدات المراجعة الداخلية الأخرى.
استناداً إلى حجم وطبيعة الجرم المزعوم والخبرة المطلوبة والموارد المتوفرة، قد يكون من المناسب أن تتولى إدارة معينة التحقيق بما يكفي لتشكيل رأي بأن عملاً إجرامياً قد ارتكب وأن يترك التحقيق اللاحق إلى الشرطة، و مناقشة هذه الأمور مع الجهات الخارجية المعنية مثل مؤسسة النقد والشرطة.

3-9-2-3 تحديث تقارير القضية :

تحديد المسؤولية بوضوح ووضع الأنظمة اللازمة لضمان المحافظة على السجلات الكاملة والتامة لجميع تقارير الاحتيال والحالات.
تحديث تقرير القضية الخاص بقضية معينة عند حدوث تغيير هام في القضية أو كل ربع سنة، أيهما أسبق.
تقع على عاتق البنك مسؤولية تحديث تقارير القضية.

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

لمؤسسة النقد أو لأي ممثل معتمد لها في أي وقت أن يطلب الإطلاع على أي تقرير قضية وأن يكون البنك المعني قادراً على تلبية هذا الطلب على الفور.

لا يلزم البنك بإجراء تحديث لاحق متى أقفل الملف، أي متى أصبح الأمر بيد القضاء أو عند إتمام العمل الإداري أو عند اتخاذ البنك قراراً بعدم اتخاذ أي تدبير لاحق.

الاحتفاظ بتقارير القضية المقفلة لمدة خمس سنوات في مكاتب البنك ويجوز بعدها تخزين هذه التقارير في أماكن نائية يمكن استردادها منها عند الطلب.

إبلاغ مؤسسة النقد عن إقفال أية قضية عندما يكون النشاط الاحتيالي المعني عند عتبة الإبلاغ أو عند تجاوزها.

3-9-2-4 تطبيق خطة التحقيق :

حيث يتخذ قرار بالتشاور مع السلطات الخارجية على الأرجح بأن يسير البنك بالتحقيق في حالة احتيال مشبوه (على الأقل حتى نقطة متفق عليها) ، وضع خطة لهذا التحقيق من البداية من قبل قائد الفريق والموافقة عليها من الإدارة العليا.

تأخذ عملية التخطيط في الاعتبار الأمور التالية.

نطاق وشروط التحقيق.

القضايا والأمور المحددة التي يجب استقصاؤها بالعمق.

تحديد المجالات التشغيلية والموظفين الرئيسيين الذين سيشتركون في التحقيق .

تحديد الخبرة المتخصصة أو المساندة المطلوبة .

الكلفة المتوقعة للتحقيق والمدة الزمنية اللازمة .

معالم المراجعة ونقاطها الرئيسية وتاريخ تقديم التقرير .

النتائج الممكنة .

التحقيق الفعّال والمؤثر في عملية احتيال كبيرة هو أمر معقد يقتضي خبرة متخصصة وموارد وقد يحتاج القيام به إلى فريق عمل من عدة اختصاصات مثل تقنية المعلومات والمحاسبة والأنظمة بالتعاون مع الشرطة. لذلك من الضروري أن يتولى التحقيق مسئولون يتمتعون بالمهارات والمعرفة المطلوبة وأن يتم تعزيز مهاراتهم بصورة مستمرة عن طريق التدريب والتطور المهني.

على قائد فريق التحقيق أن يعيد باستمرار تقييم الحاجة إلى إشراك السلطات الخارجية والتشاور معها.

إيقاف المشتبه بهم عن أداء واجباتهم أثناء التحقيق مع التفكير بعناية بتوقيت إبلاغ المشتبه به أو المشتبه بهم بذلك بالإجراءات التي يجب اتخاذها سلفاً. فقد يكون من الضروري، مثلا، أن يتولى موظف الأمن وضع الترتيبات لنقل المشتبه بهم تحت الحراسة الفعلية من موقع عمله في البنك لضمان عدم إتلاف الأدلة أو عدم إلحاق الضرر بالبنك أو بأنظمة البنك.

the case.

SAMA or any authorized representative appointed by it may at any time request to examine any case report, and the bank concerned must be able to meet this demand immediately.

A bank is not required to conduct any subsequent updating when the file is closed, i.e. as it is with the judiciary, at the completion of administrative work, or when the bank takes a decision not to take any subsequent measure.

Reports of the closed case must be kept for a period of five years at the offices of the bank, and may then be stored at remote locations where they may be recovered at request.

SAMA must be informed of the closure of any case when the concerned fraudulent activity is on the threshold of notification or exceeding it.

3-9-2-4 Application of the Investigation Plan

When a decision is taken, in consultation with external authorities, that the bank may proceed with investigating a suspected case of fraud (at least to an agreed point), a plan must be set for this investigation from the beginning by the team leader and approved by the senior management.

Planning process must take into account the following:

The scope and conditions of the investigation.

The specific issues and matters that must be investigated in depth.

Identification of operational areas and key employees who will participate in the investigation.

Identification of required specialized expertise or support.

The expected cost of the review and the length of time needed.

The features of the review, its main points and the date of submitting the report.

The possible outcomes.

Effective and efficient investigation in an act of significant fraud is a complex one, requiring specialized expertise and resources. It may need a working team of several specializations, such as information technology, accounting and law, cooperation with the police. It is therefore important that the investigation be conducted by officials with required skills and knowledge whose skills must be continuously enhanced through training and professional development.

The head of the investigation team must constantly re-evaluate the need for the participation of the external authorities and consultation therewith.

The suspected perpetrators must be banned from undertaking their duties during the investigation, but the timing of informing the suspects and the measures to be taken in a advance must be carefully considered. It may be necessary, for example, that the security officer make arrangements to transfer

the accused from his work location in the bank and put him under actual police custody to ensure the non-destruction of evidence or inflecting 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 evident 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

3-9-2-5 حماية الأدلة :

من الضروري جداً التأكد من عدم ضياع أي شكل من أشكال الأدلة أو إتلافها خلال المراحل الأولى ولدى الشرطة المهارات المتخصصة المطلوبة والمعدات للحفاظ على الأدلة وإجراء الفحوصات القضائية .

الاحتفاظ بسجل الجهات والمواقع التي يتم الحصول على الأدلة منها.

حماية المستندات الأصلية وحفظها في مكان آمن و استبدال المستندات الهامة بنسخ عنها في ملفات رسمية إذا دعت الحاجة لاستخدام الأصل في إجراء أي عمل رسمي.

عدم وضع أية علامات مميزة على المستندات الأصلية.

عدم مناولة المستندات والقطعات الورقية أو أي مستند أو وثيقة قد تشكل دليلا بل توضع ضمن غلافات بلاستيكية شفافة تسمح بقراءة المستند دون مناولته باليد. و تسجيل اسم أي شخص قام بمناولة هذه المستندات للاستخدامات التي قد تحدث مستقبلاً.

يمكن الاحتفاظ بالمعلومات الدالة الهامة على شريط طابعة، مثلا، أو على قصاصة ورقية أو في دفتر يبدو فارغاً في الظاهر. هذه البنود قد تزود الاختصاصي المتدرّب بمعلومات قيّمة ويجب بذل كل جهد ممكن لحماية هذه البنود من التلوّث.

التوثيق المهني للمباحثات الهامة مع المسئولين الرئيسيين.

يمكن العثور على الأدلة الهامة في مكتب المتهم أو في خزانة ملفاته أو في درجه المقفل أو في حقيبته اليدوية أو في سيارته. و قبل تفتيش هذه المواقع أو قبل منع الوصول إليها، يتم الحصول من الإدارة القانونية على رأيها بشأن التبعات النظامية لمثل هذا العمل وكذلك بشأن التوصل إلى الاستنتاج بأن الاتهام لم يكن مستنداً إلى أي أساس.

في حال تمّ استخدام الحاسب الآلي لارتكاب عملية احتيال يجب الحصول على رأي وتوجيه خبير قبل القيام بأية محاولة لحماية البيانات الموجودة في الحاسب الآلي أو في وسائط التخزين المعنية أو تحليلها أو حتى الدخول إليها. وقد يؤدي التقصير في اتخاذ الإجراءات الوقائية المناسبة إلى إحداث برامج تدميرية أو تدميرية ذاتية من الممكن أن تلحق أشدّ الضرر بأجهزة الحاسب الآلي أو إلى إتلاف أدلة ثبوتية هامة.

عند تقييم جوانب الاحتيال المتعلقة بالحاسب الآلي، أن تكون أولويات فريق التحقيق حماية معدات الحاسب الآلي والشبكة النظامية التي قد يكون المتهم قد دخل إليها أو من خلالها ، وذلك لضمان استمرارية العمليات والخدمات ولحماية وسائط التخزين وشفرة البرامج وغيرها من البنود التي قد تستعمل كأدلة. وقد يكون من الضروري الاستعانة بخدمات الخبراء في تدقيق الحاسب الآلي وغيرهم من الاختصاصيين

الداخليين والخارجيين لوضع وتنفيذ الضوابط للحماية.
حيث يكون مدير البيانات أو محلل الأنظمة أو خبير الشبكة أو اختصاصي تقنية المعلومات عالي المهارة، من الضروري بوجه خاص التأكد من عدم إعطاء مثل هذا الشخص أي إنذار مسبق بشأن التحقيق. وبعد التباحث مع الموظفين الكفوئين، تسحب جميع صلاحيات الدخول والوصول إلى جميع الأنظمة كأولوية أولى.

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

3-9-2-6 استرداد عائدات الاحتيال :

ملاحقة استرداد جميع الخسائر الناتجة عن الاحتيال سواء اتخذت أو لم تتخذ أية إجراءات جزائية، كما يتم إعادة تقييم أنظمة الرقابة بعد العملية لتجنب تكرارها.
يمكن ملاحقة استرداد عائدات الاحتيال والخسائر الأخرى عبر الملاحقة الجزائية أو عبر قنوات أخرى مثل العمل الإداري أو التدبير التأديبي.

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 الشرط الأساسي التاسع : معايير السلوك والإجراءات التأديبية :

3-10-1 Introduction

3-10-1 مقدمة :

على البنوك أن تطور معايير ملائمة للسلوك وتوزيعها على الموظفين والموردين والعملاء والجمهور العام. و إرسال رسالة واضحة بأنه لا تساهل مع الاحتيال وأن مرتكبيه سيتعرضون لإجراءات تأديبية.
وتشكل قواعد السلوك نقطة البداية بهذا الشأن تدعمها معايير وسياسات محددة تغطي الموظفين وتنشر مناخاً من السلوك الأخلاقي داخل البنك.
و أن تمتد هذه المعايير إلى الموظفين المتعاقد معهم وإلى المقاولين الخاصين والموردين الخاصين والاستشاريين وجميع المتعاملين مع البنك ومهامه.

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

3-10-2 الإرشادات :

على البنوك أن تطوّر معايير سلوك صالحة وأن توزعها على الموظفين والموردين والعملاء والجمهور العام.
تغطي معايير السلوك جميع فئات الموظفين داخل البنك.
تمتد هذه المعايير إلى الموظفين المتعاقدين مع البنك والمقاولين الخاصين والموردين والاستشاريين والوكلاء وأي شخص يتعامل مع البنك أو مهامه.
يمكن تفصيل معايير سلوك مختلفة أو معايير حد أدنى وإجراءات تأديبية على كامل نطاق البنك، ولكن تطبق هذه المعايير على حالات خاصة في إدارات أو أقسام معينة.

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 massage 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.

3-10-2-1 قواعد السلوك :

يساعد وضع وتوزيع قاعدة للسلوك على تحديد المعايير الأخلاقية والسلوكية للبنك. و أن تعبر قواعد السلوك السليم وأن تصف نزاهة العاملين في البنك وقيمهم الأخلاقية وكفاءتهم والسلوك الشخصي والمهني المتوقع من جميع الموظفين وفلسفة البنك وأسلوبه التشغيلي والطريقة التي تحدد فيها إدارة البنك الصلاحيات والمسؤوليات والطريقة التي تنظم بها وتطور أشخاصها والاهتمام والتوجيه الذي يوليه مجلس الإدارة لهذه المعايير.

تعزيز الرسالة الواردة في قواعد السلوك بأشكال أخرى من المستندات مثل كتيبات الموظف والإجراءات (بما في ذلك كتيب دليل بشأن مراقبة ومكافحة الاحتيال) مع التفاصيل اللازمة، والرسائل الإخبارية والتعاميم التي يمكن استخدامها لتوزيع المعايير بصورة فعّالة وتعزيزها بانتظام.

3-10-2-2 معايير التأديب :

يحدد كتيب الإجراءات التأديبية التي يقوم بها البنك ضد الموظفين الذين تثبت عليهم تهم الاحتيال.

لا يجوز لرئيس الدائرة بوجه عام أن يقبل استقالة موظف خاضع للتحقيق في قضية ما , أو موضوع له علاقة بسلوكه غير النزيه أو أي سلوك آخر يستدعي صرفه من الخدمة. ومع أن استقالة مثل هذا الموظف قد تعتبر وسيلة لتوفير الوقت والكلفة التي تنطوي عليها عملية إنهاء من الخدمة، فهنالك احتمال استمرار هذا الموظف في محاولاته الاحتيالية في مكان عمل آخر. وهذا قد يسبب حرجاً للبنك الذي سمح لهذا الشخص بالاستقالة، أو إقامة دعوى قضائية ضد البنك.

3-10-2-3 المعايير المنطبقة على الموظفين المؤقتين وموظفي الجهات الخارجية المتعاقد معها :-

تنطبق ذات المعايير المنطبقة على إدارة البنك وموظفيه على الموظفين المؤقتين وموظفي الجهات الخارجية المتعاقد معها مع البنك الذي يجب أن يدركوا ماهي تطلعات البنك الأخلاقية المنتظرة منهم. على البنوك من أجل الاستفادة القصوى من التعاقد مع الجهات الخارجية ، أن تضع أنظمة إدارة ومراقبة من شأنها أن تضبط النفقات وتخفف قدر الإمكان من الاحتيال والهدر وسوء الإدارة.

على البنك، عندما يعتمد على موارد بشرية وفنية من الخارج لتأدية بعض الخدمات له، أن يتأكد من تقييم ومراقبة موظفي الجهات المتعاقد معها ومستوى أدائهم لتحديد خطر الاحتيال وإجراءات مراقبة الاحتيال اللازمة لمكافحة واكتشاف الاحتيال.

تشكل عملية تقييم الخطر، الهادفة بصورة خاصة إلى تحديد خطر

الاحتيال الذي ينطوي عليه عقد معين، جزءًا من أعمال إدارة الخطر الموصوفة في الشرط الأساسي الثالث تحت عنوان "تقييم خطر الاحتيال". وعند تحديد المخاطر يتعين على المدراء تطوير استراتيجيات تنطبق على ذلك العقد.

تكون الاستراتيجيات الهادفة إلى تخفيف المخاطر المرتبطة بالتعاقد(outsourcing) مفصلة وأن تتضمن ترتيبات محددة للتوجيه والرقابة لضمان الإدارة المالية والمحاسبة الفعّالة ومسارات واضحة لتدقيق الحسابات.

على المدراء في سبيل تخفيف المخاطر، أن يتمتعوا بالمهارات اللازمة أو أن يتلقوا التدريب اللازم ليتمكنوا من اتخاذ القرارات المناسبة بشأن القضايا التي ينطوي عليها التعاقد.

عند إجراء عقود مع أطراف خارجية يجب أن تضمن الإدارة القانونية لدى البنك أن الإجراءات والإرشادات وتعليمات المؤسسة في هذا الخصوص قد أُخذت في الاعتبار.

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.
