AML policies

I- Regulatory and legal framework :

The concept of AML &FT was mentioned in Tunisia (member of MENAFATF) for the first time by ***law 2001-65*** dated on **10 July 2001** and replaced in August 2015 by ***organic law 2015-22***.

The implementing texts appeared firstly in 2007 by the circular 2007-07 which is replaced in 2013 by the ***circular 2013-15*** of the Central Bank of Tunisia and then in 2017 by the ***circular 2017-08***.

II- Enforcement of laws and regulations :

To be conform to the regulation, Banque de Tunisie et des Emirats had put in place a *permanent internal control system for anti-money laundering*.

The AML department provides continuous **monitoring** of profiles and operations through the **automated** system ***Siron Tonbeller***. Occasionally, the AML department receives **manual** alerts from other departments.

1- The automate Monitoring System :

A- Siron Embargo:

It allows screening through public lists (OFAC, UE and ONU) and other internal lists. It's a permanent control that blocks transactions that contains a resemblance to a watch list.

Those lists are continuously updated.

So, if it is a ***false alert***, the transaction is unblocked immediately by the AML staff.

And, if it is a ***confirmed alert***, the transaction still blocked till the ***CTAF (Commission Tunisienne des Analyses Financières)*** is informed

The module works too through **business rules** which are:

- Detecting transactions with huge amounts;
- Detecting transactions coming from countries qualified as high risk regions;
- Detecting transactions for which the beneficiary or the principal is an association;
- Detecting transactions for which the beneficiary/principal is of Libyan nationality
- Etc ...

These business rules are configurable and updated frequently.

The module detects on average **60 alerts per day.**

S.A. Au capital de TND 90 Millions - 5 bis, Rue Mohamed Badra, 1002 Tunis - RC. B140831996 - M.F.: 015094 B/A/M/000 - شركة خفية الإسم رأس مالها تسعون مليون دينار – 5 مكرر نهج محمد بدرة 1002 تونس
Fax : 71 287 409 : فاكس - Tél.: 71 112 000 : الهاتف - Swift BTE XTNTT : سويفت
Email: bte@bte.com.tn

B- Siron AML :

The automated profiling module works with **scenarios** which are:

- Nationality of the holder of the account is ...
- The name of the account holder exists in an internal list;
- Important cash transactions for a new customer;
- The account holder is an Exposed Political Person;
- The beneficial owner of the account is a PEP;
- Amount of cash payment on behalf of an association is greater than 500 DT;
- The amount of cash withdrawn from associations' accounts is greater than TND500;
- A large number of cash payments;
- Large number of cash withdrawals ;
- Country of origin or destination of funds exists on a list qualified as a high risk region;
- Significant amount of movement in flow;
- Group accounts;
- Smurfing;
- Schtrumphing;
- Short term accounts;
- Etc ...

These scenarios are up-dated every **6 months** and they detect an average of **100 alerts per day**.

Circular 2013-15 listed several indices of money laundering and terrorism financing in Annex 4. These are the main scenarios of Siron AML.

For each alert a complete analysis is made. So, the AML analysts:

- Check the alert reasons;
- Check the credentials put on the information system;
- Demand the opening folder from the agency;
- Analyse transactions;
- Ask for additional informations and explanations from the agency;
- Etc...

On the basis of the results and conclusions of the investigations, the AML officer takes one of the following decisions:

- It is a false alert and keeping the analysis folder
- It is a confirmed alert and reporting to the CTAF

For the second case, the AML officer decides to applicate an ***enhanced due diligence*** and to classify the client as a **high risk** element

C- Siron KYC :

This module has two principal functionalities which are:

- Screening the database through watch lists at the beginning of the relationship and a scan is done every month.
- The *KYC form*: in the beginning of the relationship this form has to be filled and reviewed every **six months** for high risk category and **yearly** for low and standard categories.

The **KYC form** contains all the elements of an account file:

✓ Identification of the account holder:

- **For Physical Persons:** ID card, recent bill of electricity to confirm the address etc...
- **For Entities**: Statue, trade register, tax return, ID card of shareholders, list of managers etc.

✓ Identification of the activity:

It is a primordial element to identify the client. Therefore, the Customer Advisor must have a perfect knowledge of the activity of his client.

The account manager has to verify the coherence between the information given in the beginning of the relationship and the movement of the account.

✓ Political Exposed Persons:

The automated Monitoring System allows us to identify the PEP and to classify them as **high-risk** clients. The compliance department and the CEO shall authorize starting business relationship with this category.

✓ Risk categories:

- **Law risk category** : Government establishments and other entities identified by annex 2 of the circular N°2013/15.
- **Standard risk category** : Those who do not belong to the other two categories
- **High risk category** : Associations, PEP, clients who live in non-cooperative countries, persons having a relationship with a tax haven, etc...

2- Manual Monitoring System :

In parallel with the automatic monitoring system, we have a manual system through which we receive periodic alerts from *agencies, foreign banking service staff* and *other departments*.

Circular 2013-15 imposes that the declarant describes the facts of his suspicions in a report that will be **audited** by the *external auditors*.

The AML staffs collect all the necessary information and do the investigations to qualify the declaration.

An enhanced due diligence is imposed and a new identification of the client is initiated.

- If the alert is confirmed "**a confirmed alert**", a declaration of suspicion is sent to the CTAF with all the details and necessary documents. Automatically, a new risk classification is done and the client belongs to the high-risk category.

- If it is a **false suspicion**, the report is conserved.

III- Reporting to the CTAF :

All confirmed alerts are directly and confidentially reported to the CTAF.

The declaration of suspicion must contain all the following details:

- Full identification of the suspect: name, ID card, address, etc.
- Identification of the activity
- KYC Form including the legal file
- The analysis report
- Extracts of accounts
- Details and justification of the suspicious operations.

- *CTAF Correspondents identity*:

  - The **principal declarant** :
    Full Name : Mrs. Meriem Dridi
    E-mail : meriem.dridi@bte.com.tn

  - The **alternate** :
    Full Name : Mrs. Ameni Mekni
    E-mail : ameni.mekni@bte.com.tn

IV- Operations prohibited by law :

- Anonymous accounts;
- Having a business relationship with a shell bank;
- Operating with listed persons;
- Accepting transfers from embargos;
- Sending transfers to embargos.

V- Staff Training :

Tunisian regulations impose continuous training courses for all the employees of the bank and all the branches. So, our compliance department insures at least a session per year for all the staff.

Also, compliance department diffuses, continuously, notes to all the employees to inform them about new regulations.

Training themes are:

- Identification of the customers and their activities : KYC principals
- Enhanced Due Diligences
- Risk approach
- Watch lists
- Suspicious transactions
- Etc...

Date :

Signature:

Le Directeur Général
Jalel AZZOUZ

Mr Jalel AZZOUZ
General Manager