

The Shanghai Commercial & Savings Bank, Ltd. AML/CFT Framework Summary

Introduction

The Republic of China (ROC) is a member of the Asia / Pacific Group on Money Laundering (APG) and is committed to implementing international standards to Anti- Money Laundering and Countering the Financing of Terrorism (AML/CFT) and the proliferation of mass destruction weapons with all APG members, and has formulated relevant AML/CFT laws and regulations. The effectiveness of AML/CFT mechanism has been evaluated in the Third Round Mutual Evaluation of APG in November 2018 with the best evaluation result -Regular Follow-up. The Shanghai Commercial & Savings Bank, Ltd. (SCSB) is one of the representative financial institutions participating in the evaluation, and received a very positive evaluation by the APG evaluation team.

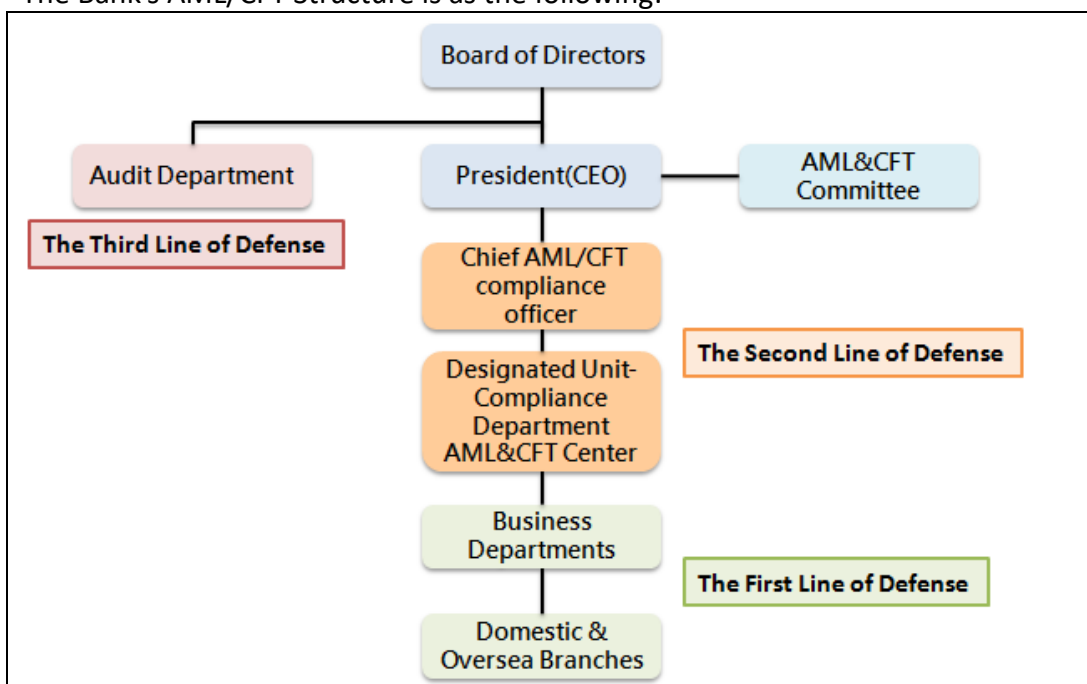
SCSB (herein referred to as the Bank) is a company registered and maintains physical presence in ROC, complying with the relevant laws and regulations of AML/CFT, and develops the Bank's AML/CFT program in accordance with FATF 40 recommendations, including AML/CFT procedures, operations and control measures, which are all under regular review. The Bank also fully cooperates with the competent authorities to prevent money laundering (ML), terrorism financing (TF) and the proliferation of mass destruction weapons, in order to fulfill the role of international financial institution as a gatekeeper.

The Bank has developed and implemented the AML/CFT program with the main objectives to:

1. Establish the principles that the Bank must follow in AML/CFT and to comply with international sanctions programs;
2. Define the respective roles and responsibilities to meet these requirements;
3. Establish the key processes that the Bank must implement; and
4. Identify the essential elements of associated governance.

Structure of AML/CFT

The Bank's AML/CFT Structure is as the following:



AML/CFT Program

The summary of the Bank's AML/CFT program is as the following, and the Bank performs institutional ML/TF risk assessment regularly, and then continuously develops and implements enhancing measures according to assessment results and the Bank's risk appetite.

1. Customer due diligence

When establishing business relationship with a customer, carrying out occasional transactions, identifying a suspicious ML/TF transaction, and having doubts about the veracity and adequacy of previously obtained customer identification data, the Bank performs Customer due diligence (CDD) and takes CDD measures as follows:

- (1) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. In addition, the Bank retains copies of the customer's identity documents or record the relevant information thereon.
- (2) Verifying that any person purporting to act on behalf of the customer is so authorized, identifying and verifying the identity of that person using reliable, independent source documents, data or information. In addition, the financial institution shall retain copies of the person's identity documents or record the relevant information thereon.
- (3) Identifying the identity of the beneficial owner of a customer and taking reasonable measures to verify the identity of the beneficial owner, including using the relevant data or information from a reliable source.
- (4) Understanding and, in view of the situation, obtaining relevant information on the purpose and intended nature of the business relationship when undertaking CDD measures.
- (5) For customers who have established business relationships non-face-to-face, besides the above measures, the Bank sets up document confirmation and relevant operations of officer identification mechanism by risk-based approach.

When performing CDD, the Bank utilizes an appropriate risk management mechanism to confirm whether the customer, its beneficial owner and senior management are PEP of domestic or foreign governments or international organizations.

The Bank also risk rating customers from an ML/TF risk perspective. The risk rating categories cover geographic, customers, products/ services, and transactions /delivery channels areas. According to these risk rating categories adopted, the Bank divides customers into 3 level-classifications (high/medium/low), and conducts periodic review to update and review customer information.

All high-risk customers (including but not limited to PEP, complex ownership/ control structure, relevant high risk industries (for example: precious stone or precious metal dealer, high value commodity agency...), high risk regions (the Bank evaluates geographic risks with reference to FATF, UN, OFAC and other relevant sources) or high risk products/services(for example: Offshore Banking Unit customers, High-Asset customers)) are required to apply enhanced CDD (EDD), and shall obtain the senior management sign-off before establishing business relationship. All high-risk customers are also subject to one-year-frequency periodic review and stricter transaction monitoring measures.

2. Watch list filtering on customers and connected parties of a transaction

Based on the risk-based approach, the Bank establishes a watch list filtering mechanism for customer and customer's connected parties, transaction-related persons, to detect, compare, and filter customer, customer's beneficial owner and senior management and transaction-related persons.

The watch list database is a purchased, professional list database, which includes 3 categories of lists, which are "Black List", "Negative News", and "PEP". Every customer, customer's beneficial owner, senior management and counter parties shall undergo watch list filtering.

The “Black List” includes the sanctioned list designated by ROC authority, the list designated by foreign governments or international organizations (for example: UN, OFAC, EU, etc.).

3. Ongoing monitoring of accounts and transactions

Based on the risk-based approach, the Bank establishes account and transaction monitoring mechanism, including setting ML/TF monitoring indicators, parameters, threshold amounts, alerts and operation procedures of monitoring, the reviewing procedures for monitored cases and reporting standards, and utilizes information system to assist in the detection of suspicious ML/TF transactions.

Besides the assistance of the system, the Bank also enhancing training continuously, in order to detect suspicious activities when facing the customer at front desk.

4. Correspondent Banking Business

The Bank has relevant procedures established for correspondent banking business including risk assessment, due diligence, and etc. The establishment of business relationship with a respondent bank requires the approval of the President of the Bank. It is forbidden to establish correspondent banking business relationships with institutions that are shell banks, or banks that allow shell banks to use their accounts, or banks involving payable through account (PTA).

5. Record-keeping

The Bank keeps records on all business relationships and transactions with customers in hard copy or electronic form for at least five years.

6. Filing currency transaction report (CTR)

The Bank reports cash transactions above a certain amount to the Investigation Bureau in a format prescribed by the Investigation Bureau via electronic media in five (5) business days after the completion of transaction.

7. Filing suspicious ML/TF transaction report (STR)

For transactions related to account, the monitoring patterns, or other situations that are deemed as suspicious ML/TF activities, the Bank completes the review process as quickly as possible to determine whether the transaction is suspected of involving ML/TF activity, and shall retain records.

Where review has resulted in a determination that a transaction is suspected of involving ML or TF activity, regardless of the amount of the transaction, the Bank promptly files a STR with the Investigation Bureau in a format prescribed by the Investigation Bureau after the report has been approved by the responsible chief compliance officer. The report shall be filed within two business days of said approval. The same shall apply to attempted (uncompleted) transactions.

8. Appointment of a compliance officer at the management level in charge of AML/CFT compliance matters

The board of directors of the Bank appoints the Executive Vice President of Compliance Department to act as chief AML/CFT compliance officer, vests the officer full authority in coordinating and supervising AML/CFT implementation. The chief AML/CFT compliance officer reports to the board of directors about material AML/CFT issues periodically.

9. Procedures for screening and hiring employees

The Bank establishes procedures for screening and hiring employees, including examining whether the prospective employee has character integrity and the professional knowledge required to perform its duty.

10. An ongoing employee training program

The Bank arranges on-boarding AML/CFT training programs for new employees and ongoing AML/CFT training programs for all staffs every year (including internal and external face to face classes, e-learning, weekly bulletin, case sharing, and etc.).

The Bank’s directors, independent directors, president, chief AML/CFT compliance

officer, the personnel of dedicated AML/CFT unit, compliance officers, internal auditors and relationship managers, every oversea and domestic branch's Senior Compliance Managers, supervisors, and AML/CFT personnel, new employees and other staff, take AML/CFT training programs according to the nature of their job characteristics.

11. An independent audit function to test the effectiveness of AML/CFT system

The Bank establishes independent internal audit system to assess whether AML/CFT program is implemented effectively. The relevant regulations of their operational procedures should be included in the self-inspection and internal audit items, and enhanced if necessary.

The Bank also appoints an independent third party to check effectiveness of AML/CFT system. The frequency of both internal audit and third party external audit is at least annually.

Conclusion

With full support of the board of directors, the Bank sets up designated AML/CFT unit, designated AML/CFT personnel, and AML/CFT supervisors in every branch/unit, and continues to implement ongoing training. The Bank also invites a professional consultant team, and includes the implementation of AML/CFT as an item of every branch and unit's compliance personnel KPI. In short, the Bank has shaped the culture from top to bottom dedicated to AML/CFT.

1. The Bank has about 5% of the Bank's total employees dedicated to AML/CFT (including the staffs in AML&CFT Center and AML/CFT supervisors in every branch/unit, etc.).
2. The Bank has continuously included the implementation of AML/CFT as an item of every branch and unit's compliance personnel KPI, and the implementation situation is reviewed and examined periodically by the AML&CFT Center in the Compliance Department, to make sure that all branches and units follow the AML/CFT program.
3. The Bank is committed to promoting AML/CFT education and training
 - (1) Encourage and tutor the Bank's employees to obtain relevant domestic and foreign licenses: As of December 31, 2019, a total of 244 people have obtained international CAMS licenses (approximately 10% of the Bank's total employees, most of which are designated AML/CFT unit staffs and AML/CFT supervisors in branch/unit), and a total of 1296 people have obtained domestic AML/CFT professional licenses (approximately 50% of the Bank's total employees).
 - (2) The AML&CFT Center records e-learning courses every year, and requires all staffs to participate in the training, along with tests after courses to check everyone's learning condition.
 - (3) There is also a weekly bulletin in the weekly morning meeting, sharing different topics of AML/CFT, including important concepts, latest news and issues, cases sharing, and etc, aiming to input AML/CFT in every staffs' DNA.
 - (4) Held a test for AML/CFT, and checked the training results of all staffs.
4. The Bank implements the review of transaction monitoring, and files STR to Investigation Bureau regarding suspicious transactions. The quality of STR filed by the Bank is better than the industry average (after filing STR, the feedback from our FIU "Distribution Rate" (i.e. the percentage of cases that the FIU has distributed to our country's prosecutors) is higher than the industry average).
5. Since 2017, the Bank has invited Deloitte & Touche's consultant team to support the establishment of the Bank's AML/CFT framework and program.
6. In November 2018, the Bank participated in the Third Round Mutual Evaluation of APG as one of the representative financial institutions. Not only did the Bank get a very positive feedback from the chairman of APG evaluation team when doing face to face meeting, the Bank also passed the on-site inspection in branches about practical operation.

