

國立臺灣大學管理學院企業管理碩士專班

碩士論文

Global MBA

College of Management

National Taiwan University

Master Thesis

洗錢防制法於金融機構的體系之應用—以花旗集團為例

Implementing Anti-Money Laundering Requirements in Financial Institutions: Evidence from  
Citigroup Inc.

何孟哲

Meng-Che Ho

指導教授：許文馨 博士

Advisor: Wen-Hsin Hsu (Audrey Hsu), Ph.D.

中華民國 112 年 5 月

May 2023



## Acknowledgement



I want to express my most profound appreciation and gratitude to the following individuals and organizations for their invaluable support and contributions to completing this thesis.

First, my advisors, Professor Wen-Hsin Hsu (Audrey Hsu) and Professor Leon van Jaarsveldt, for their guidance, mentorship, and expertise throughout the research process. Their insights, feedback, and support have been instrumental in shaping and refining this thesis.

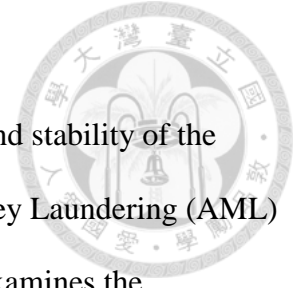
Second, my parents Ming-Shih Ho & Su-Lan Yu, supported and encouraged me during my MBA journey. Their love, understanding, and motivation have been my constant source of inspiration.

Third, our Citigroup Global Head of Markets KYC Illiano Stefano, Citigroup APAC Head of Markets KYC Malik Yashika; our Citigroup Global Markets Taiwan Securities Business Unit Manager Wilfred Ma and my friend Meng Ping Shen for their assistance and discussions during this thesis process, their constructive feedback and helpful discussions have enriched my research and improved the quality of this thesis. I am also grateful to all the authors and researchers whose works I have referenced in my thesis. Their scholarly contributions have provided the foundation for my research and have shaped my understanding of the topic.

Lastly, I want to express my heartfelt appreciation to anyone else who has supported me in any way during the completion of this thesis. Your assistance and encouragement are truly appreciated. Thank you all for your unwavering support and contributions toward completing this thesis. Your help has been invaluable, and I am deeply grateful for your presence in my academic journey.

Meng Che Ho (Mark Ho)

## Abstract

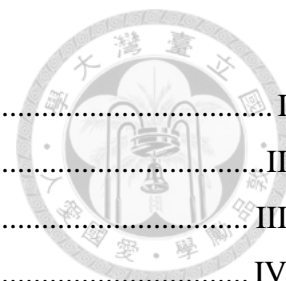


*Money laundering* is a global threat that undermines the integrity and stability of the financial system. Regulatory authorities have imposed stringent Anti-Money Laundering (AML) requirements on financial institutions to combat this menace. This thesis examines the implementation of AML requirements in Citigroup Inc., one of the largest financial institutions globally, to explore Citigroup's current practices in AML compliance management.

Through a mixed-methods approach, the thesis has combined qualitative data analysis via public sources and contributed to the existing literature on global AML standards and Taiwan AML regulations. Second, research on Citigroup's AML practices in AML compliance.

Since Citigroup is one of the largest financial institutions in the world, also Citigroup is classified as a Global Systemically Important Bank, indicating its significance and impact on the global financial system. The thesis on implementing AML requirements in Citigroup can be valuable to other financial institutions by providing insights into best practices, compliance strategies, and regulatory implications. This research can help other financial institutions strengthen their AML compliance programs, mitigate money laundering risks, and effectively comply with regulatory requirements.

## Table of Contents



|   |     |
|---|-----|
| Acknowledgement .....   | I   |
| Abstract .....  | II  |
| Table of Contents .....   | III |
| List of Tables and Figures.....   | IV  |
| List of Abbreviation .....  | V   |
| Chapter 1 Introduction .....  | 1   |
| 1.1 Research Problem .....  | 2   |
| 1.2 Research Aims and Objectives .....  | 3   |
| 1.3 Research Methodology .....  | 4   |
| 1.4 Importance and Significance of the Study .....  | 4   |
| 1.5 Structure of the Thesis .....   | 5   |
| Chapter 2 Anti-Money Laundering Standard and Related Regulations .....                    | 6   |
| 2.1 The Definition of Money Laundering.....   | 6   |
| 2.2 Anti-Money Laundering Regulations .....   | 9   |
| 2.2.1 Global AML Standard – The Financial Action Task Force (FATF) Objective.....         | 12  |
| 2.2.2 FATF 40 Recommendations .....   | 14  |
| 2.2.3 Taiwan AML Regulations.....   | 16  |
| 2.2.4 AML Penalties for Financial Institutions.....                                       | 25  |
| Chapter 3 Anti-Money Laundering Implementation at Citigroup Inc. ....                     | 26  |
| 3.1 Company Overview – Citigroup Inc.....   | 26  |
| 3.2 AML Compliance Risk Management at Citigroup.....                                      | 29  |
| 3.3 AML Internal Control Lifecycle.....   | 31  |
| 3.4 AML Program Execution - Three Line of Defense .....                                   | 38  |
| 3.5 FATF 40 Recommendations at Citigroup.....   | 43  |
| Chapter 4 Case Analysis .....   | 45  |
| 4.1 Comparison of Global AML Standard and Citigroup AML Implementation .....              | 45  |
| 4.2 Comparison of AML Taiwan Laws and Citigroup AML Implementation.....                   | 48  |
| Chapter 5 Conclusion.....   | 49  |
| References.....   | 50  |
| Appendix 1: List of the FATF 40 Recommendations.....                                      | 53  |
| Appendix 2: Wolfsberg Group Financial Crime Compliance Questionnaire by Citigroup Inc. .. | 56  |
| Appendix 3: Chinese Taipei Mutual Evaluation Report by APG.....                           | 66  |

## List of Tables and Figures

|          |                                  |
|----------|----------------------------------|
| Figure 1 | Three Stages of Money Laundering |
| Figure 2 | Citigroup Operating Segments     |
| Figure 3 | Framework of AML Program         |
| Figure 4 | Three Lines of Defense Model     |

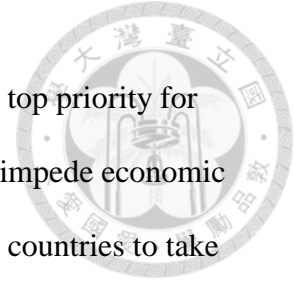


## List of Abbreviation



|             |   |
|-------------|---|
| <b>AML</b>  | Anti-Money Laundering                     |
| <b>AMLO</b> | AML Compliance Officers                   |
| <b>APG</b>  | Asia/Pacific Group on Money Laundering    |
| <b>CDD</b>  | Customer Due Diligence                    |
| <b>CTR</b>  | Currency Transaction Reports              |
| <b>CFT</b>  | Countering the Financing of Terrorism     |
| <b>EDD</b>  | Enhanced Due Diligence                    |
| <b>EMEA</b> | Europe, the Middle East, and Africa       |
| <b>FATF</b> | Financial Action Task Force               |
| <b>FIU</b>  | Financial Intelligence Unit               |
| <b>FSC</b>  | Financial Supervisory Commission          |
| <b>GCB</b>  | Global Consumer Banking                   |
| <b>ICG</b>  | Institutional Clients Group               |
| <b>MLCA</b> | Money Laundering Control Act              |
| <b>MCA</b>  | Manager Control Assessment                |
| <b>MJIB</b> | Ministry of Justice Investigation Bureau  |
| <b>NYSE</b> | New York Stock Exchange                   |
| <b>OCC</b>  | Office of the Comptroller of the Currency |
| <b>PEP</b>  | Politically Exposed Person                |
| <b>QA</b>   | Quality Assurance                         |
| <b>RBA</b>  | Risk-Based Approach                       |
| <b>STR</b>  | Suspicious Transaction Report             |
| <b>SAR</b>  | Suspicious Activity Reports               |

## Chapter 1 Introduction



The global challenge of preventing money laundering is currently a top priority for governments worldwide. This illicit activity has the ability to significantly impede economic growth and cause disruption within financial systems, making it crucial for countries to take necessary measures to safeguard their economies. Money launderers involved in fraud, corruption, or drug trafficking often use the global financial system to transfer illegal money to other entities across the globe and integrate their dirty money into clean assets.

Anti-money laundering (AML) is crucial internal control for financial institutions since anti-money laundering has been paid attention to by each country and has become a vital compliance requirement in economic systems. Financial institutions have a responsibility to comply with AML regulations to prevent their services from being exploited for illegal activities such as money laundering and terrorism financing. Furthermore, it's important to follow AML regulations to avoid facing increased regulatory restrictions, as well as potential legal consequences such as penalties and fines. For instance, in 2020, Citigroup agreed to pay \$400 million US dollars to settle the charges that US regulators fined the “Office of the Comptroller of the Currency”, and the “Federal Reserve Bureau”, given deficiencies in its risk management and AML program. The fine was related to Citigroup's failure to address ongoing deficiencies in its risk and control framework, including shortcomings in its AML program.

In addition, AML is crucial internal control to protect a reputation at financial institutions. Financial institutions must ensure they do not become associated with money laundering or other criminal activities to maintain their reputation since any negative publicity stemming from such money laundering connections can lead to a decline in the customer base and a loss of trust from the general public. Therefore, it is crucial for them to remain vigilant and

take appropriate measures to prevent any such occurrences. For example, the Deutsche Bank Moscow branch had facilitated suspicious transactions involving shell companies registered in offshore tax havens from 2010 to 2014; Deutsche bank is allowing illegal money to be laundered through its accounts without accurate detection and reporting the suspicious activities to authorities. Given this, Deutsche Bank faced reputational damage from the global money laundering scandal, including a decline in its share stock price, loss of customers, and a negative impact on its brand reputation.

Financial institutions are important in preventing illegal activities such as money laundering exposure and other financial crimes activity. By doing so, they can minimize the risk of their involvement in such activities and ensure a safe and secure financial environment globally. To comply with regulations, all financial institutions worldwide are highly recommended to implement Anti-Money Laundering risk controls effectively.

## **1.1 Research Problem**

For Financial Institutions, it's important to follow AML regulations to avoid facing increased regulatory restrictions, as well as potential legal consequences such as penalties and fines. Therefore, compliance with AML requirements is essential for financial institutions to avoid regulatory oversight, financial losses, reputational risks, and disruptions to their business operations worldwide.

The problem of this study aims to address the global AML Standards and Citigroup in implementing AML requirements in its financial institutions. Specifically, I want to address five questions: (1) What is the international AML standard? (2) What are the “Financial Action Task Force 40 Recommendations” to comply with financial institutions? (3) What are the AML rules from Taiwan Regulations? (4) What are the AML requirements that Citigroup is complying with



now? (5) What are the consequences for financial institutions if failure to follow AML regulations?



## 1.2 Research Aims and Objectives

In 2020, Citigroup agreed to pay a fine of \$400 million US dollars to settle the charges, which were fines by US regulators - the “Office of the Comptroller of the Currency”, and the “Federal Reserve Bureau”, given deficiencies in its risk management and AML program. The US regulators - the “Federal Reserve Board” and the “Office of the Comptroller of the Currency” had indicated that Citigroup's business practices have raised concerns as they may not meet safety and financial stability standards, including its deficiencies of AML controls to catch money launderers. The US regulator called Citigroup deficiencies on longstanding failure to establish effective AML risk management. As a result, it's important to follow AML regulations to avoid facing increased regulatory restrictions, as well as potential legal consequences such as penalties and fines.

During this research, the aim and objective of this thesis are to identify current global AML standards and Taiwan AML Regulations. Second, investigate the implementation of AML requirements in Citigroup Inc, assess the implementation of Citigroup's current AML practices, whether it has fulfilled global AML requirements and the effectiveness of AML compliance management in Citigroup Inc as a case study.

Since Citigroup is one of the largest financial institutions in the world, also Citigroup is classified as a Global Systemically Important Bank, indicating its significance and impact on the global financial system. The thesis on implementing AML requirements in Citigroup can be valuable to other financial institutions by providing insights into best practices, compliance strategies, and regulatory implications. This research can help other financial institutions

strengthen their AML compliance programs, mitigate money laundering risks, and effectively comply with regulatory requirements.



### **1.3 Research Methodology**

A qualitative case study methodology will be conducted to conduct a comprehensive investigation into Citigroup's Anti-Money Laundering compliance practices and application on the Global AML Standard. Primary data sources will include audited annual reports, internal policy, legal regulations, and news articles related to AML compliance. Furthermore, a case study of the analysis approach will be employed to review the collected data.

### **1.4 Importance and Significance of the Study**

The Money laundering process is illegal because criminals try to disguise their illicit funds and avoid suspicion from legal authorities. Therefore, anti-money laundering is very challenging because money laundering is a vast and potential threat in the world. Now, financial institutions, regulators, and legal authorities are working very hard to fight together for increasingly complicated criminals who are seeking to use the global financial system for illegal activity.

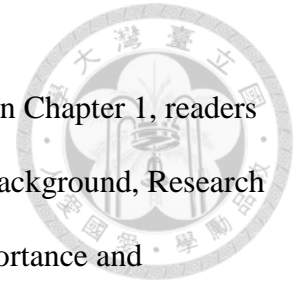
Citigroup is a well-known financial institution with a global presence and an important role in the worldwide financial system as a “Global Systemically Important Bank”. With its operations spanning over 160 countries and serving a vast customer base of over 200 million accounts, Citigroup plays a significant part in the global economy, which means, Citigroup is easy to target by money launderers and wash their dirty money via Citi’s banking system. Therefore, compliance with AML requirements is critical for Citigroup to avoid regulatory issues, financial losses, reputational risks, and disruptions to its business operations.

## 1.5 Structure of the Thesis

The thesis case study is structured into five well-defined chapters. In Chapter 1, readers can expect to find a comprehensive overview of the Introduction, Thesis Background, Research Problem, Research Aims and Objectives, Research Methodology, and Importance and Significance of the Study. Moving on to Chapter 2, there is a detailed literature review analysis. This section sheds light on the definition of money laundering, the three stages of the money laundering process, and global and Taiwan AML regulations. In addition, the AML penalties for financial institutions.

Chapter 3 focuses on the method used in the study, highlighting a company overview of Citigroup and AML implementation of Citigroup, as well as the concept of AML Compliance Risk Management, AML internal controls, and AML Program Execution. Furthermore, Implementation of “FATF 40 Recommendations” at Citigroup. Chapter 4 involves a case analysis of Citigroup, which includes evaluating its compliance with global AML requirements and comparing its AML implementation with local regulations.

Finally, in Chapter 5, readers will find a well-crafted conclusion that examines Citigroup's efforts to comply with AML requirements, including research findings, improvements, and recommendations.



## Chapter 2 Anti-Money Laundering Standard and Related Regulations



### 2.1 The Definition of Money Laundering

According to “UN Vienna 1988 Convention Article 3.1”, the definition of Money Laundering is: "the conversion or transfer of property, knowing that such property is derived from any offense(s), to conceal or disguise the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions. This means criminals generate huge illegal assets of dirty money through various illegal activities such as corruption, fraud, drug trafficking, child trafficking, extortion, etc.” However, dirty money cannot be used in the same form because there is a risk of money earned from such criminal activities coming under the scanners of law enforcement authorities. Now, illicit money is made to appear as legal assets or clean money through the laundering process. Through a series of layered transactions, the laundering process allows illicit money to be disguised and integrated into legitimate assets, effectively concealing its origin.

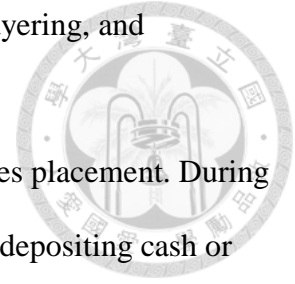
According to the money laundering definition from “United Nations Office on Drugs and Crime”, "money laundering is the processing of criminal proceeds to disguise illegal assets. The term money laundering is used because criminals try to clean their dirty money to make it appear legitimate. Money laundering can have severe consequences for financial institutions and individuals who become involved in the process. It is often difficult to detect and prosecute and can significantly drive corruption and organized crime".

The money laundering process involves criminal activity and disguising illegal assets by using the different layering of transactions at financial institutions and integrating their illicit funds into legal assets. When a criminal has generated illegal money, the criminal must find a way to use the funds without drawing the attention of legal authorities to disguise an illegal activity involved in developing such profits. Therefore, Criminals conceal the source of funds and cut connections via different layering of transactions at financial institutions so that the regulator or legal authorities cannot track the illegal funds. This means money laundering is making dirty money into clean assets.

**Figure 1: Three Stages of Money Laundering**



Money laundering is involving three stages of cycles: placement, layering, and integration, following as below descriptions:



- **Placement:** At the beginning of the money laundering process lies placement. During this stage, illegal funds are brought into the financial system by physically depositing cash or other assets into a legitimate financial institution or business. This can involve structuring transactions to evade reporting requirements, using cash-heavy businesses to make deposits, or transferring money across borders using shell companies.

- **Layering:** After illegal funds have been introduced into the financial system, the next stage of money laundering is known as layering. During this stage, the funds are separated from their illegal source and multiple layers of transactions are conducted to conceal their origin and ownership. This can be achieved through various methods such as transferring funds between accounts, converting cash into other assets, and utilizing intermediaries in different jurisdictions.

- **Integration:** The last step of money laundering is integration, where the illegal funds are made to appear as if they are legitimate funds and put back into the economy. This can be done through investing in lawful businesses, buying real estate or other assets, or carrying out legitimate transactions using laundered funds.

However, according to “United Nations Offices on Drugs and Crimes”, “money laundering cases may not have all three stages, some stages could be combined, or several stages repeat several times. For instance, Cash from drug sales is divided into small amounts, then deposited in small money and afterward transferred as payment for services to a shell company. In this case, the placement and layering are done in one stage”.

## 2.2 Anti-Money Laundering Regulations

AML regulations are designed to prevent money laundering, and AML regulations are put in place by governments and regulatory agencies to combat money laundering and other illicit financial activities. These regulations require financial institutions, including banks, securities, money service businesses, and other entities involved in financial transactions, to establish procedures to prevent illegal activity, detect transaction behavior and report any suspicious activities that may indicate money laundering. In the United States, AML regulations have expanded from “Bank Secrecy Act”<sup>1</sup>.” Bank Secrecy Act (*Bank Secrecy Act (BSA) / OCC, n.d.*)” is US legislation created in 1970 to prevent criminals from using financial institutions as tools to hide or launder their illegal assets. The law requires banks and other financial institutions to provide documentation, such as currency transaction reports to regulators. Banks can require such documentation when clients deal with suspicious cash transactions over \$10,000. The law

---

<sup>1</sup> United States Code: “Declaration of purpose of Bank Secrecy Act § 5311. (1) The global war on terrorism and cutting off terrorist financing is a policy priority for the United States and its partners, working bilaterally and multilaterally through the United Nations, the United Nations Security Council and its committees, such as the 1267 and 1373 Committees, the Financial Action Task Force (FATF), and various international financial institutions, including the International Monetary Fund (IMF), the International Bank for Reconstruction and Development (IBRD), and the regional multilateral development banks, and other multilateral fora. “(2) The international financial community has become engaged in the global fight against terrorist financing. The Financial Action Task Force has focused on the new threat posed by terrorist financing to the international financial system, resulting in the establishment of the FATF’s Eight Special Recommendations on Terrorist Financing as the international standard on combating terrorist financing. The Group of Seven and the Group of Twenty Finance Ministers are developing action plans to curb the financing of terror. In addition, other economic and regional fora, such as the Asia-Pacific Economic Cooperation (APEC) Forum, and the Western Hemisphere Financial Ministers, have been used to marshal political will and actions in support of combating the financing of terrorism (CFT) standards. “(3) FATF’s Forty Recommendations on Money Laundering and the Eight Special Recommendations on Terrorist Financing are the recognized global standards for fighting money laundering and terrorist financing. The FATF has engaged in an assessment process for jurisdictions based on their compliance with these standards. “(4) In March 2004, the IMF and IBRD Boards agreed to make permanent a pilot program of collaboration with the FATF to assess global compliance with the FATF Forty Recommendations on Money Laundering and the Eight Special Recommendations on Terrorist Financing. As a result, anti-money laundering (AML) and combating the financing of terrorism (CFT) assessments are now a regular part of their Financial Sector Assessment Program (FSAP) and Offshore Financial Center assessments, which provide for a comprehensive analysis of the strength of a jurisdiction’s financial system. These reviews assess potential systemic vulnerabilities, consider sectoral development needs and priorities, and review the state of implementation of and compliance with key financial codes and regulatory standards, among them the AML and CFT standards.” (*Bank Secrecy Act (BSA) / OCC, n.d.*)

allows authorities to more easily monitor the nature of the transactions and prevent AML risk. Also, the European Union and other jurisdictions have adopted similar measures

In Taiwan, Taiwan has established a comprehensive regulatory framework that governs the requirements for AML controls and the “Money Laundering Control Act”<sup>2</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.) provides a whole framework in Taiwan. For our financial institutions in Taiwan, every financial institution is required to follow the “Regulations Governing the Implementation of Anti-Money Laundering Programs Financial Institutions”<sup>3</sup> (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.). These laws and regulations guide specific AML requirements for financial institutions in Taiwan. Furthermore, financial institutions in Taiwan that fail to comply with AML regulations may face legal and regulatory consequences, including fines, penalties, and sanctions by “Taiwan Financial Supervisory

---

<sup>2</sup> “Article 1 of Money Laundering Control Act”: “The Act is enacted to prevent money laundering activities and combat related crimes; bolster anti-money laundering systems; maintain financial stability; increase transparency in money flows; and strengthen international cooperation.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.)

<sup>3</sup> “Article 2 of Regulations Governing the Implementation of Anti-Money Laundering Program by Financial Institutions, terms used in these Regulations are defined as follows:”

1. “Financial institution” shall mean the following banking businesses, securities and futures businesses, insurance enterprises, and other financial institutions designated by the Financial Supervisory Commission (FSC):”

(1) “Banking business includes banks, credit cooperatives, postal offices which also handle money transactions of deposit, transfer and withdrawal, bills finance companies, credit card companies and trust enterprises.”

(2) “Securities and futures business includes securities firms, securities investment and trust enterprises, securities finance enterprises, securities investment consulting enterprises, securities central depository enterprises, and futures commission merchants.”

(3) “Insurance enterprise includes insurance companies, reinsurance companies, and post offices engaging in simple life insurance business.”

(4) “Other financial institutions designated by the FSC” includes electronic payment institutions, foreign migrant worker remittance companies (limited to small-amount remittance services for foreign migrant workers), leverage transaction merchants, futures trust enterprises, and managed futures enterprises, as well as insurance agent companies, insurance broker companies, and individuals working as insurance agents and insurance brokers” (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.)



Commission”<sup>4</sup> (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.) which has the legal authority to impose administrative penalties, such as fines, and may also take legal action against financial institutions that violate AML regulations. For example, Citibank Taiwan Ltd had inadequate measures to evaluate clients' risk of money laundering and to detect suspicious transactions in 2020. Even though “Citibank Taiwan Limited” had based its AML policies on those of its US-based parent company, Citigroup Inc., however, it failed to consider transaction types specific to Taiwan that are commonly used for money laundering. Criminals in Taiwan often transfer money to China, Hong Kong, Macau, and Southeast Asian countries, which should have been highlighted the transaction system in “Citibank Taiwan Limited”. Still, the bank failed to do so because its parent company had not. As a result, the “Taiwan Financial Supervisory Commission” imposed a fine of NT\$10 million (US\$357,194) on “Citibank Taiwan Limited”, given breaches of the Taiwan AML regulations<sup>5</sup> (*Press Release-The Financial*

---

<sup>4</sup> “Article 2 of Regulations Governing the Implementation of Anti-Money Laundering Program by Financial Institutions”, “terms used in these Regulations are defined as follows”:

1. "Financial institution" shall mean the following banking businesses, securities and futures businesses, insurance enterprises, and other financial institutions designated by the Financial Supervisory Commission (FSC):

(1) "Banking business includes banks, credit cooperatives, postal offices which also handle money transactions of deposit, transfer and withdrawal, bills finance companies, credit card companies and trust enterprises.”

(2) "Securities and futures business includes securities firms, securities investment and trust enterprises, securities finance enterprises, securities investment consulting enterprises, securities central depository enterprises, and futures commission merchants.”

(3) "Insurance enterprise includes insurance companies, reinsurance companies, and post offices engaging in simple life insurance business.”

(4) "Other financial institutions designated by the FSC" includes electronic payment institutions, foreign migrant worker remittance companies (limited to small-amount remittance services for foreign migrant workers), leverage transaction merchants, futures trust enterprises, and managed futures enterprises, as well as insurance agent companies, insurance broker companies, and individuals working as insurance agents and insurance brokers”

(*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.)

<sup>5</sup> “The Financial Supervisory Commission took enforcement actions against Citibank Taiwan Limited related to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) deficiencies :

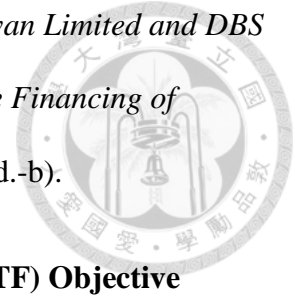
(1) Date of the penalty notice: May 13, 2021

(2) Subject of the penalty: Citibank Taiwan Limited

(3) Legal basis for the penalty: Subparagraph 7 of Article 129 of the Banking Act of the Republic of China

(4) Facts of the case: Failure to establish an effective customer risk assessment mechanism

*Supervisory Commission Took Enforcement Actions Against Citibank Taiwan Limited and DBS Bank (Taiwan) Ltd. Related to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) deficiencies-Financial Supervisory Commission, n.d.-b).*



## **2.2.1 Global AML Standard – The Financial Action Task Force (FATF) Objective**

Since money laundering was getting more severe worldwide, the G7 countries established the “Financial Action Task Force” (FATF) in 1989, an inter-governmental organization. FATF operates independently and strives to create policies that safeguard the worldwide financial system from money laundering, terrorist financing, and promote financial stability. The FATF, a global organization, has set international AML standards to encourage the efficient implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, proliferation financing, and other related threats to the integrity of the global financial system, according to the FATF Recommendations.

The FATF Recommendations are recognized worldwide as the global AML standard for implementing effective anti-money laundering and counter-terrorism financing measures at both national and international levels. Now, the “International Monetary Fund” and “World Bank” have also recognized the “FATF 40 Recommendations” as the benchmark for AML/CFT risk management globally.

---

Citibank Taiwan Ltd has major deficiencies in AML/CFT operations, including failure to establish an effective customer risk assessment mechanism, ongoing customer due diligence mechanism and transaction monitoring mechanism, insufficient implementation of customer due diligence, insufficient investigation of suspicious transaction alerts and failure to complete such investigations in a timely manner. Moreover, most of the customers or transactions involved have high-risk factors with huge transaction amounts. Based on the deficiencies, it was found that the bank has not properly established or sufficiently implemented its internal AML/CFT control mechanism and process, in violation of Article 7 of the Money Laundering Control Act and Article 45-1 of the Banking Act of the Republic of China. According to Article 24 of the Administrative Penalty Act, the bank was fined NT\$10 million in accordance with Subparagraph 7 of Article 129 of the Banking Act of the Republic of China." (*Press Release-The Financial Supervisory Commission Took Enforcement Actions Against Citibank Taiwan Limited and DBS Bank (Taiwan) Ltd. Related to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) deficiencies-Financial Supervisory Commission, n.d.-b)*)

As of 2023, 39 countries and territories are members of the “Financial Action Task Force” (FATF), along with regional organizations that implement the “FATF 40 recommendations”. “The FATF member countries are following as below: Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, the European Union, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Ireland, Israel, Italy, Japan, South Korea, Luxembourg, Malaysia, Mexico, the Netherlands, New Zealand, Norway, Portugal, the Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, the United Kingdom, the United States, the United Arab Emirates, and Saudi Arabia”.



The FATF does not possess an authority to impose fines or penalties on member countries that refuse to comply with its recommendations. Nevertheless, the organization has introduced a policy that utilizes "**Peer Pressure**" to encourage each member country to adhere to its guidelines. This approach includes requesting progress reports at the meetings and even suspension of membership. Turkey, a member of the FATF since 1990, was the first country to be subjected to the Peer Pressure in 1996 due to its failure to criminalize money laundering and inadequate laundering controls. Turkey responded by enacting a money laundering law just a month later.

Every member country of FATF plays a crucial role in the organization's commitment to fighting financial crime and preserving the integrity of the worldwide financial system.

## 2.2.2 FATF 40 Recommendations

The FATF organization was established by G7 countries to combat the misuse of financial systems for drug money laundering in 1989. In 1990, they created the FATF Forty Recommendations and revised in 1996 to adapt to evolving money laundering methods and expand their scope beyond drug money laundering. In 2001, the FATF expanded to address the funding of terrorist activities and organizations, developing the Eight (later Nine) Special Recommendations on Terrorist Financing. These recommendations have been updated several times and endorsed by over 180 countries as the global AML standard for AML/CFT. Recently, in February 2012, the FATF proposed new measures to prevent the spread of weapons of mass destruction and created a new list of “FATF 40 Recommendations” (**Appendix 1**). Now the “FATF 40 Recommendations” have been classified as a blueprint in global AML standards and provide a comprehensive framework to combat the AML and CFT measures. Therefore, the FATF Recommendations establish an international standard each country should implement through actions tailored to their specific circumstances.

Financial institutions have a crucial role in carrying out the recommendations outlined by FATF 40 Recommendation since these recommendations have a significant impact on financial institutions. Here is a form of “FATF 40 Recommendations”:

- AML/CFT Policies and Cooperation
- Money Laundering and Confiscation
- Terrorist Financing and Finance of Proliferation
- Preventive Measures: (1) Customer due diligence, (2) Record keeping, (3) Additional measures for specific customers and activities, (4) Reliance, Controls

and Financial Groups, (5) Reporting of suspicious transactions, (6) Designated non-financial Businesses and Professions (DNFBPs)

- Transparency and Beneficial Ownership of Legal Persons and Arrangements
- Powers and Responsibilities of Competent Authorities and Other Institutional Measures: (1) Regulation and Supervision, (2) Operational and Law Enforcement, (3) General Requirements, (4) Sanctions
- International Cooperation

To summarize, financial institutions are significantly impacted by the “FATF 40 recommendations”. They are required to enforce strong AML and CFT measures, carry out comprehensive customer due diligence, report any suspicious transactions activity, maintain client documentation, and invest in their employees, internal systems, and technology to comply with the latest global AML standards. Failure to follow these recommendations can lead to reputational risk and financial institutions' business loss.

### 2.2.3 Taiwan AML Regulations

Taiwan has implemented AML measures in line with global AML standards recommended by the FATF origination. The implementation of these measures for financial bodies is overseen and supervised by the “**Taiwan Financial Supervisory Commission**” (金融監督管理委員會).



From Taiwan’s legal basis perspective, Taiwan has implemented a comprehensive regulatory framework governing anti-money laundering requirements: the “**Money Laundering Control Act**”<sup>6</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b) and “**Regulations Governing the Anti-Money Laundering of Financial Institutions**”<sup>7</sup> (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b) provides an overarching framework for AML measures in Financial Institutions. For the “Money Laundering Control Act” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), financial institutions must implement risk-based AML measures, including CDD/EDD, documents keeping, and suspicious transactions reports. For “Regulations Governing Anti-Money Laundering of Financial Institutions” (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China*

---

<sup>6</sup> “Article 1 of Money Laundering Control Act”: “The Act is enacted to prevent money laundering activities and combat related crimes; bolster anti-money laundering systems; maintain financial stability; increase transparency in money flows; and strengthen international cooperation.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

<sup>7</sup> “Article 1 of Regulations Governing Anti-Money Laundering of Financial Institutions”: “These Regulations are enacted pursuant to the first part of Paragraph 4, Article 7, Paragraph 3 of Article 8, Paragraph 3 of Article 9 and Paragraph 3 of Article 10 of the Money Laundering Control Act” (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

(Taiwan), n.d.-b), this regulation has described more specific AML requirements and best practices for financial institutions.



There is a key element from Taiwan's "Money Laundering Control Act" (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b) and "Regulations Governing the Anti-Money Laundering of Financial Institutions" (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b):

- **Scope of Application:** According to "Article 5 of the Money Laundering Control Act"<sup>8</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), "The act applies to all individuals and legal entities involved in financial transactions, including financial institutions, insurance companies, securities firms, and money changers". Moreover, "the phrase financial institution encompasses banking establishments, securities and futures firms, insurance companies, and other financial institutions" authorized by the "Taiwan Financial Supervisory Commission" (金融監督管理委員會) according to "Article 2 of Regulations Governing Anti-Money Laundering of Financial Institutions"<sup>9</sup> (*Regulations Governing Anti-Money*

---

<sup>8</sup>"Article 5 of the Money Laundering Control Act": "As used in this Act, financial institutions include: Banks; Trust and investment corporations; Credit cooperative associations; Credit departments of farmers' associations; Credit departments of fishermen's associations; Agricultural Bank of Taiwan; Postal institutions handling postal savings, remittance businesses and simple life insurance business; Bills finance companies; Credit card companies; Insurance companies; Securities companies; Securities investment trust enterprises; Securities finance enterprises; Securities investment consulting enterprises; Centralized securities depository enterprises; Futures commission merchants; Trust enterprises; and Other financial institutions designated by the competent authorities in charge of the relevant industries." (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

<sup>9</sup> "Article 2 of Regulations Governing Anti-Money Laundering of Financial Institutions": "Financial institution shall mean the following banking businesses, securities and futures businesses, insurance enterprises, and other financial institutions designated by the Financial Supervisory Commission (FSC):"

*Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b).

- **Customer Due Diligence:** According to “Article 7 of the Money Laundering Control Act”<sup>10</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), Financial institutions are required to establish and implement risk-based methods to identify and verify their customers, understand their business activities, and assess their potential money laundering or terrorist financing risks. In addition, according to “Article 3 of Regulations Governing the Anti-Money Laundering of Financial Institutions” (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), the law has provided more specific details for the AML Program. It’s important to ensure compliance with customer due diligence requirements, financial institutions must implement the following measures:

---

(1) "Banking business includes banks, credit cooperatives, postal offices which also handle money transactions of deposit, transfer and withdrawal, bills finance companies, credit card companies and trust enterprises."

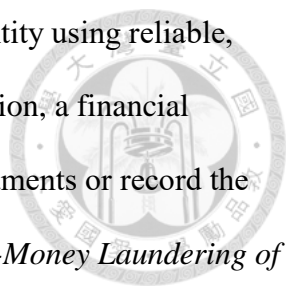
(2) "Securities and futures business includes securities firms, securities investment and trust enterprises, securities finance enterprises, securities investment consulting enterprises, securities central depository enterprises, and futures commission merchants."

(3) "Insurance enterprise includes insurance companies, reinsurance companies, and post offices engaging in simple life insurance business."

(4) "Other financial institutions designated by the FSC" includes electronic payment institutions, foreign migrant worker remittance companies (limited to small-amount remittance services for foreign migrant workers), leverage transaction merchants, futures trust enterprises, and managed futures enterprises, as well as insurance agent companies, insurance broker companies, and individuals working as insurance agents and insurance brokers (hereinafter referred to as insurance agents and insurance brokers)" (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

<sup>10</sup>Article 7 of the Money Laundering Control Act": “Financial institutions and designated nonfinancial businesses or professions shall apply a risk-based approach to undertake customer due diligence measures for verifying the identity of the customer and beneficial owner, and keep all information obtained through the customer due diligence measures.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)



- 
- “Identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information. In addition, a financial institution shall retain copies of the customer’s identity documents or record the relevant information thereon”. (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)
  - “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”. (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)
  - “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”. (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)
  - “Understanding and, in view of the situation, obtaining relevant information on the purpose and intended nature of the business relationship when undertaking CDD measures”<sup>11</sup> (*Regulations Governing Anti-Money Laundering of Financial*

---

<sup>11</sup>“Article 6 of Regulations Governing Anti-Money Laundering of Financial Institutions”: “A financial institution shall determine the extent of applying CDD and ongoing due diligence measures under Subparagraph 4 of Article 3 and the preceding article based on a risk-based approach (RBA)”:

1. “For higher risk circumstances, a financial institution shall perform enhanced CDD or ongoing due diligence



- **Record Keeping:** According to “Article 7 of the Money Laundering Control Act”<sup>12</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan), n.d.-b*), Financial institutions must maintain records of their CDD/ EDD process, transactions, and suspicious activities for a minimum period should be available for review by regulatory authorities. In addition, according to “Article 12 of Regulations Governing Anti-Money Laundering of Financial Institutions” (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan), n.d.-b*), it is necessary for

---

measures, including adopting at least the following additional enhanced measures:

- (1) Obtaining the approval of senior management before establishing or entering a new business relationship;
- (2) Taking reasonable measures to understand the sources of wealth and the source of funds of the customer. The aforementioned source of funds refers to the substantial source from which the funds generate; and
- (3) Conducting enhanced ongoing monitoring of the business relationship.

2. For customers from high ML/TF risk countries or regions, a financial institution shall conduct enhanced CDD measures commensurate with the risks identified.

3. For lower risk circumstances, a financial institution may apply simplified CDD measures, which shall be commensurate with the lower risk factors. However simplified CDD measures are not allowed in any of the following circumstances:

- (1) Where the customers are from or in countries and jurisdictions known to have inadequate AML/CFT regimes, including but not limited to those which designated by international organizations on AML/CFT as countries or regions with serious deficiencies in their AML/CFT regime, and other countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT as forwarded by the FSC; or

- (2) Where there is a suspicion of ML/TF in relation to the customer or the transaction.

The provisions of Items (1) and (2) of Subparagraph 1 of the preceding paragraph do not apply to stored value card registration operation.

An insurance enterprise should include the beneficiary of a life insurance policy as a relevant risk factor in determining whether to apply enhanced CDD measures. If the insurance enterprise determines that a beneficiary who is a legal person or a trustee presents a higher risk, it should take enhanced CDD measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout.” (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan), n.d.-b*)

<sup>12</sup>“Article 7 of the Money Laundering Control Act”: “The information obtained through the customer due diligence measures prescribed in the preceding paragraph shall be maintained for at least five years after the business relationship is ended, or after the date of the occasional transaction, unless a longer record-keeping term is required by other laws.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan), n.d.-b*)

financial institutions to maintain transaction records and KYC records for **at least five years**. In certain cases, they may have to hold onto these records for a longer duration depending on other legal obligations.



- **Reporting Requirements:** According to “Article 10 of the Money Laundering Control Act”<sup>13</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b) and “Article 15 of Regulations Governing Anti-Money Laundering of Financial Institutions”<sup>14</sup> (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), financial institutions are required to report suspicious transactions activity to the “**Taiwan Ministry of Justice Investigation**

---

<sup>13</sup>“Article 10 of the Money Laundering Control Act”: “Financial institutions and designated nonfinancial businesses or professions shall report to the Investigation Bureau of the Ministry of Justice all suspicious transactions, including attempted transactions, which may involve any of the offenses described in Articles 14 and 15. Financial institutions and designated nonfinancial businesses or professions, including responsible persons, directors, managers and employees of such institutions or businesses reporting suspicious transactions as prescribed in the preceding paragraph shall be exempted from business confidentiality obligations.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

<sup>14</sup>“Article 15 of Regulations Governing Anti-Money Laundering of Financial Institutions”: “Financial institutions shall file suspicious ML/TF transaction reports in accordance with following provisions:

1. For a transaction that exhibits the monitoring patterns or other irregularities set out under Subparagraph 5 of Article 9 herein, a financial institution shall complete the review process as quickly as possible in accordance with the provisions of Subparagraphs 4 and 6 of that same articles to determine whether the transaction is suspected of involving ML/TF activity, and shall retain records.
2. 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, a financial institution shall promptly file an STR with the Investigation Bureau in a format prescribed by the Bureau after the report has been approved by the responsible chief compliance officer at the institution. The report shall be filed within two business days of said approval. The same shall apply to attempted transactions.
3. For obviously significant suspicious ML/TF transactions of urgent nature, a financial institution should file a report as soon as possible to the Investigation Bureau by fax or other feasible means and follow it up with a written report. The financial institution is not required to submit a follow-up written report, provided the Investigation Bureau has acknowledged the receipt of report by sending a reply by fax. In such event, the financial institution shall retain the faxed reply.
4. The formats of STR and faxed reply mentioned in the preceding two subparagraphs shall be prescribed by the Investigation Bureau.
5. The data reported to the Investigation Bureau and relevant transaction records shall be kept in accordance with Article 12.”

**Bureau**” (法務部調查局) for all suspicious transactions, including any transactions that may be related to money laundering or terrorist financing.

- **Internal Controls and Compliance Programs:** According to “Article 6 of the Money Laundering Control Act”<sup>15</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), Financial institutions must establish and implement internal controls and compliance programs to ensure their operations comply with Taiwan local regulation.
- **Training and Awareness:** According to “Article 6 of the Money Laundering Control Act”<sup>16</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), Financial institutions must provide AML training or relevant courses to their current employees and raise awareness of AML issues.
- **Criminalization of Money Laundering:** According to “Article 14 of the Money Laundering Control Act”<sup>17</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), Money laundering is a criminal offense with established penalties, including fines and imprisonment. Those guilty of money laundering can face up to **seven years in prison and a fine of no more**

---

<sup>15</sup>“Article 6 of the Money Laundering Control Act”: “Each of the financial institutions and the designated nonfinancial businesses or professions shall establish its own internal control and audit system against money laundering based on the risk of money laundering and terrorism financing as well as business scale.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

<sup>16</sup>“Article 6 of the Money Laundering Control Act”: “Regular on-the-job training for money laundering prevention organized or attended by the financial institution.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

<sup>17</sup>“Article 14 of the Money Laundering Control Act”: “Anyone involved in money laundering activities prescribed in paragraphs in Article 2 shall be sentenced to imprisonment of not more than seven years; in addition, a fine of not more than NT\$ 5 million shall be imposed.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

**than NT\$ 5 million.** It is essential to take action against criminals involved in such illegal activities.

- **Supervision and Enforcement:** According to “Article 6 of the Money Laundering Control Act”<sup>18</sup> (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), the act is enforced by the “Ministry of Justice, R.O.C” (中華民國法務部) and the “Taiwan Financial Supervisory Commission” (金融監督管理委員會), who are responsible for supervising and enforcing compliance with the regulation by financial institutions. In addition to the “Money Laundering Control Act” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), Taiwan's AML framework is further supported by other more specific regulations, the “Regulations Governing Anti-Money Laundering of Financial Institutions” (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b), the regulation provides additional guidance on specific AML requirements and AML risk management for financial institutions in Taiwan .

---

<sup>18</sup>“Article 6 of the Money Laundering Control Act”: “The central competent authorities in charge of the relevant industries shall conduct regularly inspections of the implementation of the system prescribed in the preceding paragraph, and may delegate the inspections to another agency, institution, legal person or organization to do so. The central competent authorities in charge of the relevant industries shall, in consultation with the Ministry of Justice and other relevant government agencies, establish the regulations governing performance content, operating procedures, implementation measures prescribed in paragraph 1, the method of inspection and review , the qualification and conditions of delegation prescribed in preceding paragraph, and other matters to be obeyed; consultation with relevant industry associations shall be held prior to the establishment of the regulations.” (*Money Laundering Control Act - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-b)

Taiwan is not a member of the “Financial Action Task Force” (FATF), but Taiwan (Chinese Taipei) is a member of the “Asia Pacific Group on Money Laundering” (APG), which is an APAC regional body that aims to prevent money laundering and terrorist financing in the Asia-Pacific region. As part of its membership in the APG, Taiwan undergoes an annual review to assess its compliance with AML controls. The most recent APG Evaluation Report for Taiwan (Chinese Taipei) was published in September 2019; the report assesses Taiwan's AML compliance with global standards as set out by the FATF and evaluates the effectiveness of Taiwan's AML/CFT framework.

Overall, the APG Evaluation report published in 2019 (**Appendix 3**) indicated that Taiwan (Chinese Taipei) had a good understanding of AML/CFT risks and that its relevant legal framework was strong and well-developed. The report noted that Taiwan had made significant progress in improving its AML/CFT framework since its last evaluation in 2007, including the introduction of new regulations, the establishment of a financial intelligence unit, and the development of a risk-based approach to AML/CFT in Taiwan<sup>19</sup> (*Asia / Pacific Group on Money Laundering*, n.d.-b).

---

<sup>19</sup> “The Asia/Pacific Group on Money Laundering (APG) is an inter-governmental organization consisting of 41 members in the Asia-Pacific region, as well as organizations, and observers from outside the region. Under Article 1 of the APG Terms of Reference 2012, the APG is a non-political, technical body, whose members are committed to the effective implementation and enforcement of the internationally accepted standards against money laundering, financing of terrorism and proliferation financing set by the Financial Action Task Force. This document, any expression herein, and/or any map included herein, are without prejudice to the status of, or sovereignty over, any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Under the APG Terms of Reference, membership in the APG is open to jurisdictions which have a presence in the Asia-Pacific region.” (*Asia / Pacific Group on Money Laundering*, n.d.-b)

## 2.2.4 AML Penalties for Financial Institutions

It's important to follow AML regulations to avoid facing increased regulatory restrictions, as well as potential legal consequences such as penalties and fines.

Some examples of penalties and sanctions imposed by legal authorities on financial institutions for AML violations are:

- Deutsche Bank: In 2017, Deutsche Bank faced a fine of \$630 million in 2017 by both U.K. and U.S. authorities for its inability to prevent suspicious transactions activity and worth \$10 billion from being laundered out of Russia.
- Standard Chartered: In 2019, Standard Chartered was fined \$1.1 billion by U.S. legal authorities due to lack of AML controls and AML violations.
- JPMorgan Chase: In 2020, JPMorgan Chase was fined \$920 million to settle charges related to AML failures. U.S. legal authorities “fined the penalty, including the “Department of Justice, the “Commodity Futures Trading Commission”, and the “Securities and Exchange Commission”.
- Citigroup Inc: Citigroup agreed in January 2020 to pay \$400 million to the “Office of the Comptroller of the Currency”. The penalty was imposed because weaknesses in its AML risk management and Citi’s internal controls concerning its AML program.



## Chapter 3 Anti-Money Laundering Implementation at Citigroup Inc.



### 3.1 Company Overview – Citigroup Inc.

Based in New York, USA, Citigroup Inc. is a well-known global financial services firm that emerged in 1998. Citigroup is a globally recognized financial institution that provides advanced financial services and Citigroup is listed on the “New York Stock Exchange”, and its inclusion in the “S&P 500” index highlights its significant impact globally.

Furthermore, Citigroup operates through a network of subsidiaries and branches in different jurisdictions, including the United States, Asia Pacific, Europe, the Middle East, and Africa. Citigroup also operates in Taiwan through two legal entities: “Citibank Taiwan Limited” (花旗台灣商業銀行) and “Citigroup Global Markets Taiwan Securities Company Limited” (花旗環球證券股份有限公司) with powerful earning ability.

In 2022, Citigroup earned revenue of 75.34 billion dollars globally, and the company employs more than 200,000 people worldwide, and its significant competitors are JPMorgan Chase, Bank of America, Morgan Stanley, and Goldman Sachs.

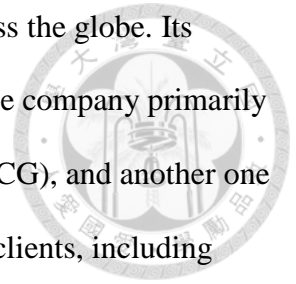


Refer to the table below for a brief overview of Citigroup's history:

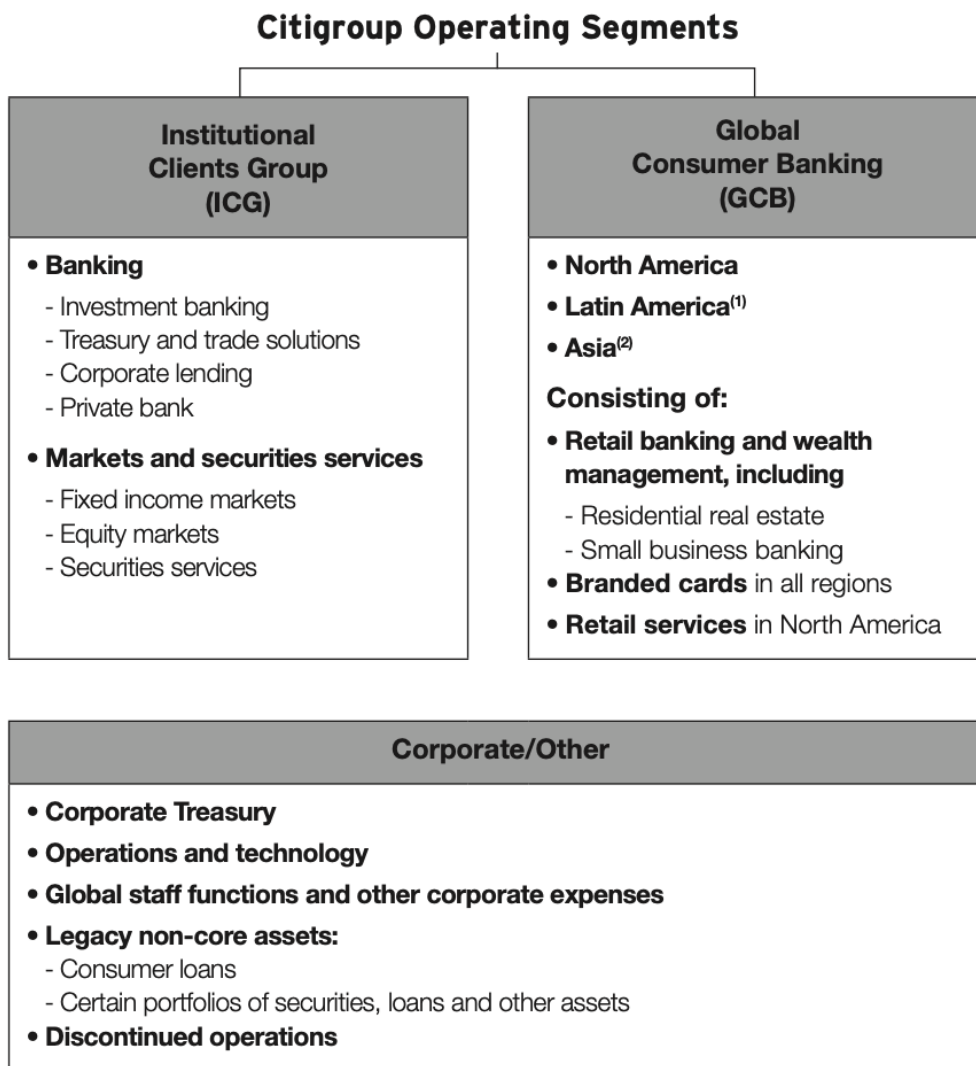


| Year | Event   |
|------|---|
| 1812 | The City Bank of New York, which would later become Citibank, is established in New York City.  |
| 1863 | The First National City Bank of New York is chartered as a national bank.   |
| 1897 | The bank is renamed to The National City Bank of New York.  |
| 1919 | The bank establishes its international presence with the opening of its first foreign branch in Buenos Aires, Argentina.  |
| 1930 | The bank merges with The First National Bank of New York, becoming The First National City Bank of New York.  |
| 1955 | The bank introduces its first credit card, the "Charge-It" card, which later becomes the Diners Club card.  |
| 1967 | The bank adopts the name "Citibank" to reflect its international presence.  |
| 1998 | Citicorp, the parent company of Citibank, merges with Travelers Group to form Citigroup Inc., creating one of the world's largest financial services conglomerates. |
| 2008 | Citigroup receives a bailout from the U.S. government during the global financial crisis.   |
| 2012 | Michael Corbat becomes CEO of Citigroup Inc.  |
| 2020 | Citigroup Inc. announces Jane Fraser as its new CEO, making her the first female CEO of a major Wall Street bank.   |
| 2021 | Citigroup Inc. announces plans to exit several consumer banking markets outside the U.S. to focus on its core businesses.   |

Citigroup offers a wide range of financial services to customers across the globe. Its services include banking, investment banking, and wealth management. The company primarily operates through two business lines: one is “Institutional Clients Group” (ICG), and another one is “Global Consumer Banking” (GCB). First, ICG focuses on institutional clients, including corporations, governments, and financial institutions. It provides a business with investment banking, capital markets, and securities services. Second, GCB focuses on retail customers and provides a business such as general deposit accounts and loans product with retails customers.



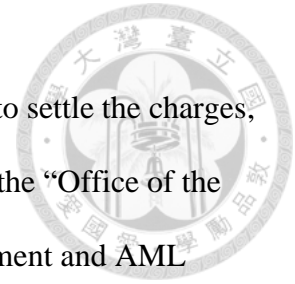
**Figure 2: Citigroup Operating Segments**



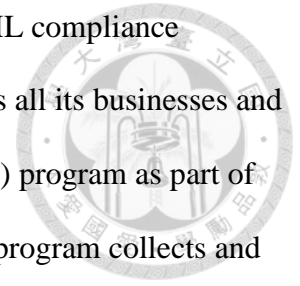
### 3.2 AML Compliance Risk Management at Citigroup

In 2020, Citigroup agreed to pay a fine of \$400 million US dollars to settle the charges, which were fines by US regulators, “Federal Reserve Bureau” (FRB), and the “Office of the Comptroller of the Currency” (OCC), given the lack of AML risk management and AML program. The US regulators - the “Federal Reserve Board” and the “Office of the Comptroller of the Currency” had indicated that Citigroup was doing business for unsafe and unsound banking practices, including its deficiencies of AML controls to catch money launderers. The US regulator called Citigroup deficiencies on longstanding failure to establish effective AML risk management.

According to the Risk Compliance Management perspective from Citigroup 2021 Annual Report Page 60, “Citi is required to interpret and implement extensive and frequently changing regulatory and legislative requirements in the U.S. and other jurisdictions in which it does business, resulting in substantial compliance, regulatory, and other risks, and costs. In addition, there are heightened regulatory scrutiny and expectations in the U.S. and globally for large financial institutions, as well as their employees and agents, concerning governance, infrastructure, data, and risk management practices and controls. These requirements and expectations also include, among other things, those related to customer and client protection, market practices, anti-money laundering, and sanctions. **A failure to comply with these requirements and expectations or resolve any identified deficiencies could result in increased regulatory oversight and restrictions, enforcement proceedings, penalties, and fines**”. (*Citi | Investor Relations | Citi Annual Reports*, n.d.)



Over the past few years, Citigroup has been paying attention to AML compliance management and implementing many regulatory changes worldwide across all its businesses and functions. Citigroup has implemented the “**Know Your Customer**” (KYC) program as part of its commitment to maintaining a secure financial environment. This KYC program collects and maintains client information to establish a thorough and effective global Anti-Money Laundering risk management control. The KYC program is critical to promoting financial stability and transparency in Citigroup.



### 3.3 AML Internal Control Lifecycle

At Citigroup, AML Compliance Risk Management is highly prioritized as it stabilizes the framework for carrying out crucial aspects of the AML program throughout three stages of the AML Control Lifecycle: Prevention, Detection, and Reporting (*Citi / Anti-Money Laundering*, n.d.-c). See the following description:

**Figure 3: Framework of AML Program**


| Prevention  | Detection   | Reporting  |
|---|---|--|
| Account Opening <ul style="list-style-type: none"> <li>• Customer Identification Program</li> <li>• Know Your Customer (KYC) Processes</li> <li>• Enhanced Due Diligence</li> </ul> Customer Screening<br>Training<br>Policies and Procedures<br>Risk Assessments | Transaction Monitoring <ul style="list-style-type: none"> <li>• Alert Generation</li> <li>• Investigations</li> </ul> Client Behaviour Profiling<br>Periodic Reviews<br>Enterprise-wide Reviews | Suspicious Activity Reporting<br>Account Restrictions or Closures<br>Business Reviews<br>Management Information<br>Risk Analysis |

- Prevention:** According to Citigroup AML Compliance Risk Management Implementation, “Building and adhering to a strong Know Your Customer (KYC) program through customer due diligence that focuses on the creation and administration of globally consistent standards/policies, customer risk scoring, onboarding, and maintenance of customer data housed in an enterprise-wide repository” (*Citi / Anti-Money Laundering*, n.d.-c).

According to Citigroup Global AML Know Your Customer Policy, “Customer Due Diligence (CDD) is the process of obtaining and reviewing sufficient information about a customer to reasonably assess the AML and terrorist financing risks associated with the customer, taking into account the customer’s products, services, and expected activity. This assessment process facilitates the assignment of a Risk Rating to the customer and determines the appropriate level of ongoing scrutiny required. In addition, clients that

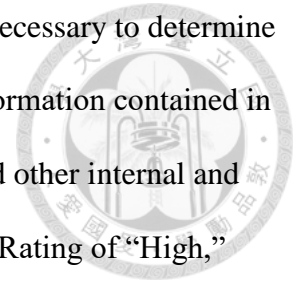
pose higher money laundering and terrorist financing risks are subject to enhanced scrutiny or Enhance Due Diligence (EDD). This enhanced level of scrutiny is not a one-size-fits-all, but rather, a risk-based approach designed to provide Citi with a more comprehensive understanding of the risks associated with the client, as well as confirmation of factual information provided by the client, in order to mitigate the risks presented. The appropriate level of due diligence, including any necessary EDD, is based on the results of the CDD completed on the customer. EDD may be required based on responses to certain customer due diligence questions on the KYC Form that indicate higher risk or may be based on the Risk Rating. Further, certain types of clients are generally recognized to pose a higher risk, and accordingly, are also subject to EDD. As part of the Know Your Customers (KYC) process, the Client Owner (Anyone with responsibility for the client, including the Relationship Manager, Responsible Party, Financial Analyst, Financial Advisor, or Customer Team) must obtain the following minimum information”:

- Geography: The client’s location, citizenship or place of incorporation, location of wealth and assets, and planned locations for establishing and conducting banking activity with Citi.
- Business/Employment: Employment information for customers that are Individuals and the type, nature, and history of the business/organization for customers that are Entities.
- Finances: Information about affluence, including assets and investments, annual revenue or income, and source of wealth or income.

- 
- Beneficial Ownership: Identification information on any Beneficial Owners in accordance with their structure.
  - Senior Public Figures (SPF) Status: Information about whether the client (or Beneficial Owner, close associate, or immediate family member of the client) is, or has ever been affiliated with a government in a significant capacity.
  - Reputation: Reputational information, especially related to criminal or ethical allegations, charges, or convictions, and any relevant reputational information from any previous relationship with Citi.
  - Product Profile: Information on the customer's planned banking activity and whether the customer plans to use high-risk products. If the customer engages in high-risk products additional information is required.

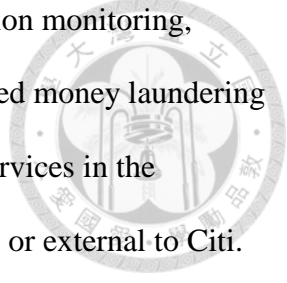
**Once Citi has received the client's KYC information, this is necessary to process background checks through an internal screening tool.** The Client Owner, with support from Operations, Investigative Units, and other support functions, is responsible for screening activities, and the Client Owner is responsible for the escalation of Sanctions matches and final disposition of any Name Screening matches, as required by this Policy and related Policies. Screening results, including the disposition of any matches, are captured in the client's KYC Profile. Screening is required for the client and associated Individuals and Entities, including the Accountholder, Beneficial Owner, or other parties related to a customer's account(s) that have been identified as part of Customer Due Diligence (CDD) / Enhanced Due Diligence (EDD).

Further, at onboarding and throughout the client relationship, it is necessary to determine and subsequently reassess the client's Risk Rating based on the information contained in the KYC Profile, rules applicable to the associated Client Type, and other internal and external factors that may be relevant. Each client must have a Risk Rating of "High," "Medium," or "Low," with the High-Risk band further refined into "High-High," "High-Medium," and "High-Low." **A client is assigned one of these five Ratings based on the client's AML customer risk score.**



- **Detection:** According to Citigroup AML Compliance Risk Management Implementation, "Global transaction monitoring to identify unusual or suspicious transactions or patterns of activity, as well as robust Global AML Investigations to provide holistic reviews of both new and existing clients across various businesses and regions" (*Citi / Anti-Money Laundering*, n.d.-c). In addition, according to Citigroup Global AML Transaction Monitoring Policy, transaction monitoring measures have been addressed as below:
  - Citi is responsible for managing money laundering risk enterprise-wide for the purpose of detecting and reporting money laundering, terrorist financing, and other illicit activities. The scale and scope of Citi's Businesses in terms of their customer base, the wide range of complex products offered, the high volume of transactions processed, and the international geographic footprint introduce money laundering risks that Citi mitigates through detection protocols, which are executed either through automated means or alternative transaction monitoring measures.



- 
- Citi employs a risk-based approach to AML transaction monitoring, meaning that monitoring is performed where identified money laundering risks are presented by its customers, products, and services in the facilitation of financial transactions, whether internal or external to Citi. Certain products and services do not require AML transaction monitoring, due to either the nature of the risk profile (e.g., those which facilitate deals such as Mergers & Acquisitions, security underwriting, and strategic financing as opposed to transaction-based activities) or the mitigation of risks through other AML controls (e.g., Prevention related activities).
  - Citi addresses its regulatory detection and reporting obligations through In-Business AML transaction monitoring programs and Compliance functions in the second line of defense. Citi's AML transaction monitoring programs are designed to address the regulatory requirements set forth by the firm's primary regulators. In accordance with regulatory expectations, Citi Businesses regulated by the "Office of the Comptroller of the Currency" and designated as "High Risk" at the inherent risk level as per Citi's Enterprise-Wide AML Risk Assessment require AML transaction monitoring to be executed through Citi's Strategic AML DCI Program. When determining the AML transaction monitoring approach for a Business, additional consideration is given to the nature of the Business and product/services offered, transactional volumes processed, and existing compensating controls and transaction monitoring processes, as relevant.

- **Reporting:** According to Citigroup AML Compliance Risk Management Implementation, actively creating, maintaining, and filing “Suspicious Activity Reports” and “Suspicious Transaction Reports” to regulators or legal authorities is essential for maintaining a safe financial environment (*Citi / Anti-Money Laundering*, n.d.-c). Further, according to Citigroup Global AML Transaction Monitoring Policy, AML transaction monitoring is executed to identify unusual activity and patterns of activity or transactions to determine whether “Suspicious Activity Reports” or “Suspicious Transaction Reports” (collectively, “regulatory filings”) should be filed, or other actions should be taken to protect Citi from risk. The purpose of these requirements is to create enterprise-wide consistency in detecting and addressing money laundering transaction risk in order to minimize the potential for financial losses, increased legal or compliance expenses, and reputational risk to the firm while ensuring the presence of an effective AML program strategy. In Taiwan as an example, **financial institutions are required to report suspicious transactions to the “Taiwan Ministry of Justice Investigation Bureau” (法務部調查局) all suspicious transactions** based on “Article 15 of Regulations Governing Anti-Money Laundering of Financial Institutions”<sup>20</sup> (*Regulations Governing*

---

<sup>20</sup>“Article 15 of Regulations Governing Anti-Money Laundering of Financial Institutions”: “Financial institutions shall file suspicious ML/TF transaction reports in accordance with following provisions:

1. For a transaction that exhibits the monitoring patterns or other irregularities set out under Subparagraph 5 of Article 9 herein, a financial institution shall complete the review process as quickly as possible in accordance with the provisions of Subparagraphs 4 and 6 of that same articles to determine whether the transaction is suspected of involving ML/TF activity, and shall retain records.
2. 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, a financial institution shall promptly file an STR with the Investigation Bureau in a format prescribed by the Bureau after the report has been approved by the responsible chief compliance officer at the institution. The report shall be filed within two business days of said approval. The same shall apply to attempted transactions.
3. For obviously significant suspicious ML/TF transactions of urgent nature, a financial institution should file a report as soon as possible to the Investigation Bureau by fax or other feasible means and follow it up with a written report. The financial institution is not required to submit a follow-up written report, provided the Investigation Bureau has acknowledged the receipt of report by sending a reply by fax. In such event, the financial institution shall retain the faxed reply.”

*Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-c), including any transactions that may be related to money laundering or terrorist financing. Therefore, Citigroup’s affiliates in Taiwan – “Citibank Taiwan Limited” and “Citigroup Global Markets Taiwan Securities Company Limited” are necessary to report to the “Taiwan Ministry of Justice Investigation Bureau” (法務部調查局) if there is any suspicious transaction activity happened.

---

4. The formats of STR and faxed reply mentioned in the preceding two subparagraphs shall be prescribed by the Investigation Bureau.

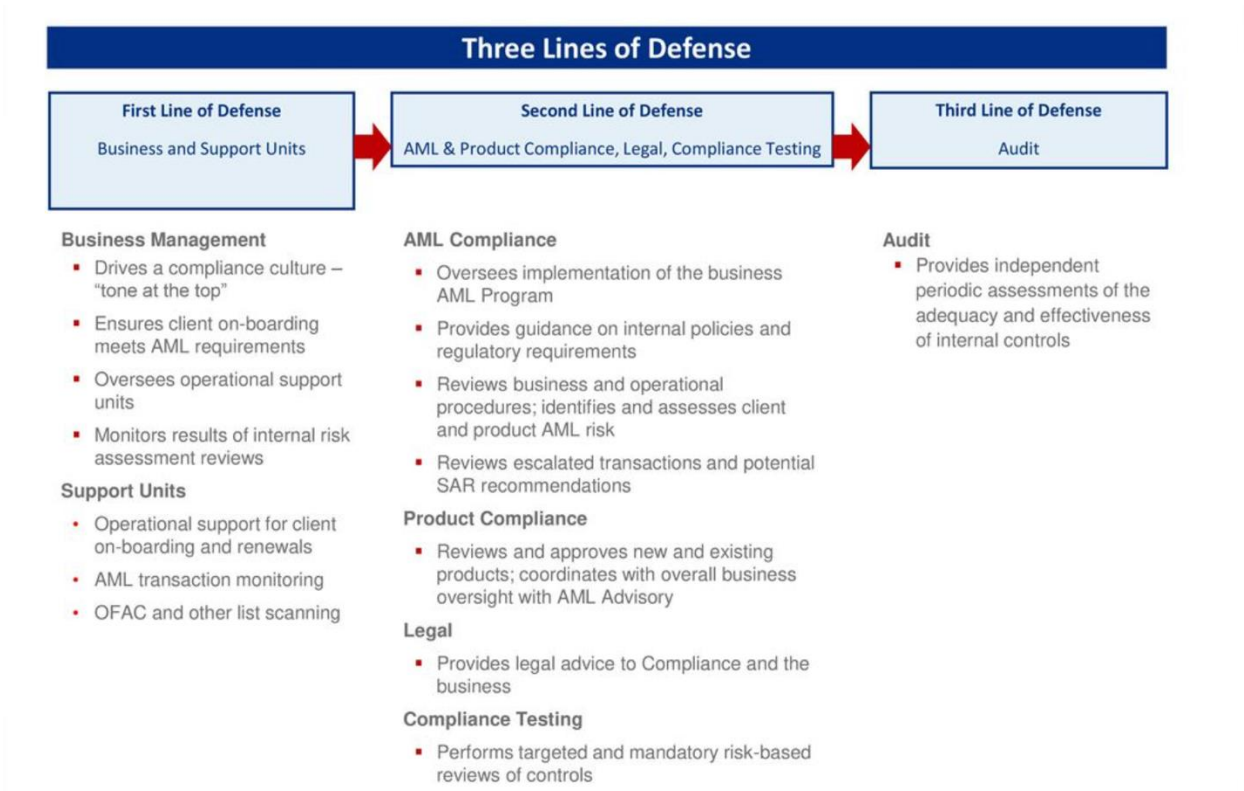
5.” The data reported to the Investigation Bureau and relevant transaction records shall be kept in accordance with Article 12.” (*Regulations Governing Anti-Money Laundering of Financial Institutions - Article Content - Laws & Regulations Database of the Republic of China (Taiwan)*, n.d.-c)

### 3.4 AML Program Execution - Three Line of Defense

According to AML Compliance Risk Management Implementation, Citigroup implements an AML risk management framework that operates under a three-line defense strategy (*Citi / Anti-Money Laundering*, n.d.-c), outlined as follows:

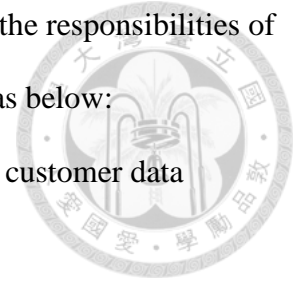


**Figure 4: Three Lines of Defense Model**



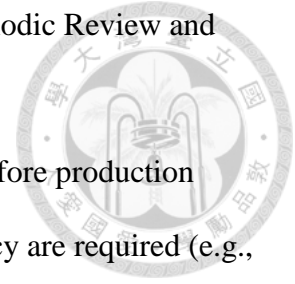
- First Line of Defense (Business & Support Units Functions)** - According to AML Compliance Risk Management Implementation, “each of Citi's Businesses, including in-Business risk personnel, owns and manages the risks, including compliance risks, inherent in or arising from the Business, and is responsible for having controls in place to mitigate key risks, performing manager assessments of internal controls, and promoting a culture of compliance and control” (*Citi / Anti-Money Laundering*, n.d.-c). Further,

according to Citigroup Global AML Know Your Customer Policy, the responsibilities of the first line of defense-related KYC/AML Controls are following as below:



- KYC Profiles: Quality, collection, and ownership of customer data throughout the client relationship.
- Client Risk Awareness: Evaluation and acceptance of risk at onboarding, Scheduled Review, and at any time during the client relationship when the client's KYC Profile changes.
- Name Screening: Dispositioning Senior Public Figure "SPF," "Watch List" or "Adverse Media" screening matches.
- Escalations: Raising to AML, and where appropriate, Global Sanctions, any material AML and Sanctions risk issues discovered during the creation or maintenance of the KYC Profile. In addition, all matters involving client-related behavior that is unusual or evasive and that is identified during the creation or maintenance of the KYC profile, or during the lifecycle of a client relationship, are expected to be referred to AML.
- Cross-Sector Clients: Identifying higher-risk clients that are shared by more than one Business and establishing, apportioning, and recording in the KYC Profile the responsibilities of each relevant business related to the maintenance of due diligence records and the coordination of Scheduled Reviews.
- Controls: Establishing, implementing, and verifying controls, including the Quality Assurance (QA) process, Manager Control Assessment

(MCA) process, client onboarding controls, and Periodic Review and Client Refresh cycle controls.



- Impact Assessments: Performing impact analysis before production changes are implemented when changes to this Policy are required (e.g., Methodology reassessments). Once Policy has been updated, provide evidence of the business' readiness to comply with new/revised requirements as part of the Implementation Assessment.
- Training: Providing training to Business and Operations personnel on the requirements of this Policy, as appropriate to their roles and responsibilities, in coordination with the respective AML Training Representative and in accordance with the Global AML, Sanctions and Anti-Bribery and Corruption Training Standard.
- **Second Line of Defense (Independent Control Functions)** - According to AML Compliance Risk Management Implementation, "Citi's independent control functions, including Compliance, Finance, Legal and Risk, set standards according to which Citi and its businesses are expected to manage and oversee risks, including compliance with applicable laws, regulatory requirements, policies, procedures, and standards of ethical conduct. In addition, the independent control functions provide advice and training to Citi's Businesses and establish tools, methodologies, processes, and oversight of controls used by the Businesses to foster a culture of compliance and control and to satisfy those standards. AML Advisory and Coverage AML Compliance Officers support their respective business by providing regulatory compliance expertise and guidance in an

advisory capacity to Business Management. They are responsible for coordinating, monitoring, and, where appropriate, overseeing day-to-day compliance with the Global AML Program” (*Citi / Anti-Money Laundering*, n.d.-c). Therefore, according to Citigroup Global AML Know Your Customer Policy, the responsibilities of the second line of defense-related KYC/AML Controls are following as below:

- Program Oversight: Overseeing the development and implementation of KYC policies, standards, processes, and procedures, including risk methodologies and CitiKYC and other systems change requests reviewing and determining the disposition of implementation plans and extension requests and acting as an escalation point for any KYC program issues.
- Exception Requests Approval: Reviewing and determining the disposition (final approval/denial) of exception requests for local law requirements.
- Risk Methodology: Maintenance of the Methodology, including critical inputs and periodic re-assessment to incorporate emerging industry-wide AML risks and those particular to Citi’s evolving customer base and product offerings.
- Control Events: Maintenance of High-Risk Account Classification, Material Change Event monitoring, and batch screening (Batch Screening) configurations (e.g., rules, thresholds) and periodic re-assessment to incorporate emerging industry-wide AML risks and those particular to Citi’s evolving customer base and product offering.
- Global KYC Standards and Forms: Maintenance of the Global KYC “Standards” and “Forms,” including a periodic re-assessment to address

emerging industry-wide AML risks and those particular to Citi's evolving customer base and product offerings, and periodically assessing the consistent application of the standards across the organization.

- Program Effectiveness Review: The management process for supporting the Global KYC Program elements to ensure the quality and reliability of KYC execution.
- Temporary Waivers: Confirming account restrictions are in place for accounts suspended due to temporary waiver expiration.

- **Third Line of Defense (Internal Audit)** - According to AML Compliance Risk Management Implementation, "Citi's Internal Audit function independently reviews activities of the first two lines of defense based on a risk-based audit plan and methodology approved by the Citigroup Board of Directors." (*Citi / Anti-Money Laundering*, n.d.-c)



### 3.5 FATF 40 Recommendations at Citigroup

The FATF Recommendations are recognized worldwide as the standard for implementing effective anti-money laundering and counter-terrorism financing measures at both national and international levels. The IMF and World Bank have also recognized these recommendations as the ultimate benchmark for combating money laundering and terrorist financing globally.

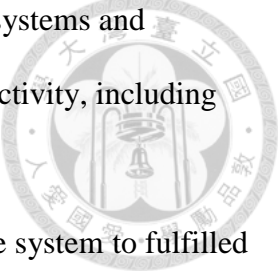
To comply with the “FATF 40 Recommendations” at Citigroup, “Wolfsberg Group Financial Crime Compliance Questionnaire”<sup>21</sup> (*wolfsberg-principles.com*, n.d.) is a valuable tool that it can assist financial institutions in detecting potential areas of weakness in their AML/CFT frameworks, as well as in determining compliance with the FATF Recommendations.

According to “Wolfsberg Group Financial Crime Compliance Questionnaire” by Citigroup Inc., which signed by Citigroup Global Senior Compliance Manager Jacqueline Sanjuas on May 2021 (**Appendix 2**), Citigroup Inc. and its affiliates have implemented a range of measures and identified it on “Wolfsberg Group Financial Crime Compliance Questionnaire”, including below significant points:

- **Customer Due Diligence:** Citigroup Inc. conducts CDD to identify and verify (ID&V) of its customers, understand the nature of business and purpose of their business relationships, and assess the risk controls of AML/CFT.
- **Enhanced Due Diligence:** Citigroup Inc. conducts EDD on customers and transactions that are considered high-risk exposure, such as politically exposed persons (PEPs) and high-value transactions.

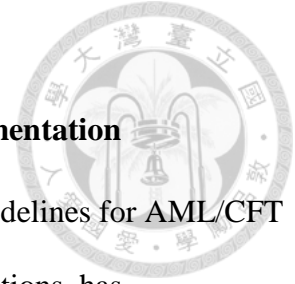
---

<sup>21</sup>“Wolfsberg Group is an association of global financial institutions, including Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank and UBS.” (*wolfsberg-principles.com*, n.d.)

- 
- **Transaction Monitoring:** Citigroup Inc. uses complicated internal systems and processes to monitor customer transactions and identify suspicious activity, including those related to AML/CFT exposure.
  - **Internal Controls:** Citigroup Inc. has implemented a comprehensive system to fulfilled internal controls to detect, prevent, report the risks of AML/CFT.
  - **Employee Training:** Citigroup Inc. provides a regular training to its employees to ensure they understand their roles and responsibilities in preventing AML/CFT.

Overall, Citigroup Inc. has implemented a strong AML/CFT framework that is targeted to fulfill the “FATF 40 Recommendations” and other applicable regulations in its business jurisdictions.

## Chapter 4 Case Analysis



### 4.1 Comparison of Global AML Standard and Citigroup AML Implementation

The FATF is an international organization that sets policies and guidelines for AML/CFT measures. Citigroup, as a financial institution operating in multiple jurisdictions, has implemented its own AML controls by the FATF recommendations, and the AML program has been addressed in “Wolfsberg Group Financial Crime Compliance Questionnaire”. Therefore, there is an analysis and comparison of whether Citigroup has fulfilled FATF Recommendations, as shown in the following table.

Overall, Citigroup’s AML program is designed to meet and exceed the FATF recommendations and is regularly reviewed and updated to ensure compliance with evolving regulatory requirements.

|     | “FATF Recommendations”  |              | “Wolfsberg Group Financial Crime Compliance Questionnaire by Citigroup Inc.”   | Answer |
|-----|---|--------------|--|--------|
| 1-2 | <p><b>“AML/CFT Policies and Coordination”</b></p> <ul style="list-style-type: none"> <li>“Assessing risks and applying a risk-based approach”</li> <li>“National cooperation and coordination”</li> </ul> | 23, 24,      | <ul style="list-style-type: none"> <li>“Does the due diligence process result in customers receiving a risk classification?”</li> <li>“Does the Entity have a risk-based approach to screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?”</li> </ul>  | Yes    |
| 3-4 | <p><b>“Money Laundering and Confiscation”</b></p> <ul style="list-style-type: none"> <li>“Money laundering offenses”</li> <li>“Confiscation and provisional measures”</li> </ul>                          | 15a, 29, 39b | <ul style="list-style-type: none"> <li>“Has the Entity documented policies and procedures consistent with applicable AML, CTF &amp; Sanctions regulations and requirements to reasonably prevent, detect and report?”</li> <li>“Does the Entity have risk-based policies, procedures and monitoring processes for the identification and reporting of suspicious activity? Examples of different forms of money laundering, terrorist financing and</li> </ul> | Yes    |

|       |  |                            |   |     |
|-------|--|----------------------------|---|-----|
|       |  |                            | sanctions violations relevant for the types of products and services offered”   |     |
| 5-8   | <p><b>“Terrorist Financing and Financing of Proliferation”</b></p> <ul style="list-style-type: none"> <li>• “Terrorist financing offenses”</li> <li>• “Targeted financial sanctions related to terrorism and terrorist Financing”</li> <li>• “Targeted financial sanctions related to proliferation”</li> <li>• “Non-profit organizations”</li> </ul>  | 15b, 35, 39b               | <ul style="list-style-type: none"> <li>• “Has the Entity documented policies and procedures consistent with applicable AML, CTF &amp; Sanctions regulations and requirements to reasonably prevent, detect and report?”</li> <li>• “Does the Entity have policies, procedures or other controls reasonably designed to prohibit and / or detect actions taken to evade applicable sanctions prohibitions, such as stripping, or the resubmission and / or masking, of sanctions relevant information in cross border transactions?”</li> <li>• “Examples of different forms of money laundering, terrorist financing and sanctions violations relevant for the types of products and services offered”</li> </ul> | Yes |
| 9-23  | <p><b>“Financial and Non-Financial Institution Preventative Measures”</b></p> <ul style="list-style-type: none"> <li>• “Financial institution secrecy laws”</li> <li>• “Customer due diligence and record-keeping”</li> <li>• “Additional measures for specific customers and activities”</li> <li>• “Reliance, controls and financial groups”</li> <li>• “Reporting of suspicious transactions”</li> <li>• “Designated non-financial businesses and professions”</li> </ul> | 21, 18, 9m, 9o, 29, 30, 31 | <ul style="list-style-type: none"> <li>• “Which of the following does the Entity gather and retain when conducting CDD? Select all that apply”</li> <li>• “Does the Entity have a record retention procedure that comply with applicable laws?”</li> <li>• “Transaction Monitoring”</li> <li>• “Suspicious Activity Reporting”</li> <li>• “Does the Entity have risk-based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?”</li> <li>• “What is the method used by the Entity to monitor transactions for suspicious activities?”</li> <li>• “Does the Entity have regulatory requirements to report suspicious transactions?”</li> </ul>              | Yes |
| 24-25 | <p><b>“Transparency and Beneficial Ownership of</b></p>  | 22a, 22                    | <ul style="list-style-type: none"> <li>• “Ultimate beneficial ownership”</li> <li>• “Are ultimate beneficial owners verified?”</li> </ul>   | Yes |

|         |  |                |   |     |
|---------|--|----------------|---|-----|
|         | <p><b>Legal Persons and Arrangements</b></p> <ul style="list-style-type: none"> <li>• “Transparency and beneficial ownership of legal persons”</li> <li>• “Transparency and beneficial ownership of legal arrangements”</li> </ul>   | a1, 33         | <ul style="list-style-type: none"> <li>• “Does the Entity adhere to the Wolfsberg Group Payment Transparency Standards?”</li> </ul>   |     |
| 26 - 35 | <p><b>“Powers and Responsibilities of Competent Authorities and Other Institutional Measures”</b></p> <ul style="list-style-type: none"> <li>• “Regulation and supervision”</li> <li>• “Operational and law enforcement”</li> <li>• “General requirements Sanctions”</li> </ul>                                      | 15, 34b, 39, d | <ul style="list-style-type: none"> <li>• “Has the Entity documented policies and procedures consistent with applicable AML, CTF &amp; Sanctions regulations and requirements to reasonably prevent, detect and report”</li> <li>• “Local Regulations”</li> <li>• “New issues that occur in the market, e.g., significant regulatory actions or new regulations”</li> </ul>  | Yes |
| 36 - 40 | <p><b>International Cooperation</b></p> <ul style="list-style-type: none"> <li>• “International instruments”</li> <li>• “Mutual legal assistance”</li> <li>• “Mutual legal assistance regarding freezing and confiscation”</li> <li>• “Extradition”</li> <li>• “Other forms of international cooperation”</li> </ul> | 34a, 37a - 37e | <ul style="list-style-type: none"> <li>• “FATF Recommendation 16”</li> <li>• “Consolidated United Nations Security Council Sanctions List (UN)”</li> <li>• “United States Department of the Treasury's Office of Foreign Assets Control (OFAC)”</li> <li>• “Office of Financial Sanctions Implementation HMT (OFSI)”</li> <li>• “European Union Consolidated List (EU)”</li> <li>• “Lists maintained by other G7 member countries”</li> </ul> | Yes |

Note: The tables are data analysis and comparison of “FATF 40 Recommendations” and “Wolfsberg Group Financial Crime Compliance Questionnaire” by Citigroup Inc. that Citigroup Global Senior Compliance Manager Jacqueline Sanjuas signed off on May 2021.

## 4.2 Comparison of AML Taiwan Laws and Citigroup AML Implementation

Citigroup's AML implementation is designed to comply with AML regulations, including those doing business in Taiwan, given Citigroup has an affiliate in the jurisdiction – “Citibank Taiwan Limited” and “Citigroup Global Markets Taiwan Securities Company Limited”, and is subject to regular internal and external audits to ensure compliance. For Taiwan, primary AML law is the “Money Laundering Control Act” and also “Regulations Governing Anti-Money Laundering of Financial Institutions”.

Citigroup's AML implementation is based on a risk-based methodology, which is consistent with the Taiwan AML requirement for financial institutions to assess the money laundering risk calculation associated with their customers and transactions activity. Citigroup's AML implementation also includes customer due diligence, enhanced due diligence, documents-keeping at least five years, and suspicious transactions activity reports, which are key elements from the Taiwan “Money Laundering Control Act” and also “Regulations Governing the Anti-Money Laundering of Financial Institutions”. It is worth to mentioning that the “Money Laundering Control Act” and also “Regulations Governing the Anti-Money Laundering of Financial Institutions” are comprehensive legal frameworks with specific country requirements that may differ from those of other jurisdictions.

In summary, while Citigroup's AML implementation is designed to comply with global AML standards and local regulations, including the Taiwan “Money Laundering Control Act” and also “Regulations Governing the Anti-Money Laundering of Financial Institutions”, a detailed assessment of Citigroup's specific requirements is needed to comply with local regulations.

## Chapter 5 Conclusion

In conclusion, implementing anti-money laundering (AML) requirements in financial institutions is critical in ensuring the financial stability and preventing illegal economic activities. Also, this study highlights the importance of continuous improvement in AML compliance efforts for financial institutions and the importance of detecting, preventing, and reporting on money laundering activities. At the same time, this case study is focused on Citigroup and examines its efforts to comply with AML risk management.

The research is indicated that Citigroup has made significant efforts to implement AML requirements, including developing internal policies and procedures, providing training to employees, and implementing technology systems on money laundering activities. However, there are still areas where improvements can be made, including AML compliance risk management, quality assurance control, and internal workflow controls. **i.e., Enhance Maker / Checker / Approver in each function.**

It is recommended that Citigroup continue to invest in AML compliance efforts and mitigate any potential risk to business activities. This will help to ensure that they remain effective in preventing money laundering activities and compliant with AML requirements.

## References



*Bank Secrecy Act (BSA) & Anti-Money Laundering (AML) Examinations / OCC. (n.d.).*

*<https://www.occ.treas.gov/topics/supervision-and-examination/bsa/bsa-aml-examinations/index-bsa-aml-examinations.html>*

*Citi | Anti-Money Laundering. Retrieved*

*from <https://www.citigroup.com/citi/citizen/antimoneylaundering/index.htm>*

*Citigroup Inc. (2021) annual report. Retrieved from*

*<https://www.citi.com/citi/investor/quarterly/2022/annual-report/>*

*Flitter, E. (2019, April 10). Standard Chartered Fined \$1.1 Billion for Violating Sanctions and Anti-Money Laundering Laws. The New York Times. Retrieved*

*from <https://www.nytimes.com/2019/04/09/business/standard-chartered-sanctions-violations.html>*

*Flitter, E. (2021, February 10). Citigroup is fined \$400 million over 'longstanding' internal problems. The New York Times. Retrieved*

*from <https://www.nytimes.com/2020/10/07/business/citigroup-fine-risk-management.html>*

*JPMorgan Chase & Co. Agrees To Pay \$920 Million in Connection with. (2020, September 29).*

*Retrieved from <https://www.justice.gov/opa/pr/jpmorgan-chase-co-agrees-pay-920-million-connection-schemes-defraud-precious-metals-and-us>*

*John J. Byrne (2016). CAMS Examination Study Guide. Retrieved from*

*[https://www.aml101.com/CAMS\\_Study\\_Guide.pdf](https://www.aml101.com/CAMS_Study_Guide.pdf)*



*Money laundering. (n.d.). United Nations: UNODC ROMENA. Retrieved from <https://www.unodc.org/romena/en/money-laundering.html>*



*Money Laundering Control Act, ROC, §5 (2018) Retrieved from <https://mojlaw.moj.gov.tw/ENG/LawContentE.aspx?LSID=FL006664>*

*Money Laundering Control Act, ROC, §6 (2018) Retrieved from <https://mojlaw.moj.gov.tw/ENG/LawContentE.aspx?LSID=FL006664>*

*Money Laundering Control Act, ROC, §7 (2018) Retrieved from <https://mojlaw.moj.gov.tw/ENG/LawContentE.aspx?LSID=FL006664>*

*Money Laundering Control Act, ROC, §10 (2018) Retrieved from <https://mojlaw.moj.gov.tw/ENG/LawContentE.aspx?LSID=FL006664>*

*Money Laundering Control Act, ROC, §14 (2018) Retrieved from <https://mojlaw.moj.gov.tw/ENG/LawContentE.aspx?LSID=FL006664>*

*Press Release-The Financial Supervisory Commission took enforcement actions against Citibank Taiwan Limited and DBS Bank (Taiwan) Ltd. related to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) deficiencies-Financial Supervisory Commission. (n.d).*

*[https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0,2&mcustomize=multimessage\\_view.jsp&dataserno=202105270002&dtable=News](https://www.fsc.gov.tw/en/home.jsp?id=54&parentpath=0,2&mcustomize=multimessage_view.jsp&dataserno=202105270002&dtable=News)*

*Regulations Governing Anti-Money Laundering of Financial Institutions, ROC, (2021), Retrieved from <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380252>*

*Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission, ROC, (2021) Retrieved from <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380262>*



*Schuetze, K. F. A. (2017, January 31). Deutsche Bank fined \$10 billion sham Russian trades. U.S. Retrieved from <https://www.reuters.com/article/us-deutsche-mirrortrade-probe-idUSKBN15FIGT>*

*The FATF Recommendations. Retrieved from <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>*

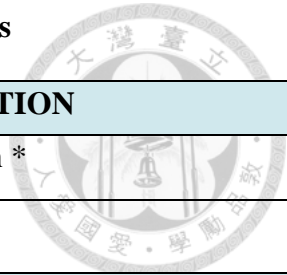
*The FATF Country List (n.d.). Retrieved from <https://www.fatf-gafi.org/en/countries/fatf.html>*

*United Nations: Office on Drugs and Crime. Retrieved from <https://www.unodc.org/unodc/en/money-laundering/index.html?ref=menuse>*

*UN Vienna (1988). Convention Article 3.1. Retrieved from [https://www.unodc.org/pdf/convention\\_1988\\_en.pdf](https://www.unodc.org/pdf/convention_1988_en.pdf)*

*VIRITHA, B. (2016). Anti-money laundering practices in Banks: Customer's awareness and acceptance in India. *Journal of Money Laundering Control*, 19(3), 8–8. doi:10.1108/jmlc-03-2015-0009*

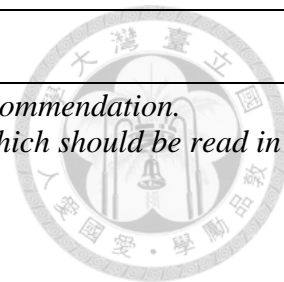
## Appendix 1: List of the FATF 40 Recommendations



|    |             |   |
|----|-------------|---|
|    |             | <b>A – AML/CFT POLICIES AND COORDINATION</b>                                |
| 1  | -           | Assessing risks & applying a risk-based approach *                          |
| 2  | R.31        | National cooperation and coordination *                                     |
|    |             | <b>B – MONEY LAUNDERING AND CONFISCATION</b>                                |
| 3  | R.1 & R.2   | Money laundering offence *  |
| 4  | R.3         | Confiscation and provisional measures *                                     |
|    |             | <b>C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION</b>               |
| 5  | SRII        | Terrorist financing offence *   |
| 6  | SRIII       | Targeted financial sanctions related to terrorism and terrorist financing * |
| 7  |             | Targeted financial sanctions related to proliferation *                     |
| 8  | SRVIII      | Non-profit organizations *  |
|    |             | <b>D – PREVENTIVE MEASURES</b>  |
| 9  | R.4         | Financial institution secrecy laws  |
|    |             | <i>Customer due diligence and record keeping</i>                            |
| 10 | R.5         | Customer due diligence *  |
| 11 | R.10        | Record keeping  |
|    |             | <i>Additional measures for specific customers and activities</i>            |
| 12 | R.6         | Politically exposed persons *   |
| 13 | R.7         | Correspondent banking *   |
| 14 | SRVI        | Money or value transfer services *  |
| 15 | R.8         | New technologies *  |
| 16 | SRVII       | Wire transfers *  |
|    |             | <i>Reliance, Controls and Financial Groups</i>                              |
| 17 | R.9         | Reliance on third parties *   |
| 18 | R.15 & R.22 | Internal controls and foreign branches and subsidiaries *                   |
| 19 | R.21        | Higher-risk countries *   |
|    |             | <i>Reporting of suspicious transactions</i>                                 |

|    |             |  |
|----|-------------|--|
| 20 | R.13 & SRIV | Reporting of suspicious transactions *   |
| 21 | R.14        | Tipping-off and confidentiality  |
|    |             | <b><i>Designated non-financial Businesses and Professions (DNFBPs)</i></b>                       |
| 22 | R.12        | DNFBPs: Customer due diligence *   |
| 23 | R.16        | DNFBPs: Other measures *   |
|    |             | <b>E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS</b>               |
| 24 | R.33        | Transparency and beneficial ownership of legal persons *   |
| 25 | R.34        | Transparency and beneficial ownership of legal arrangements *                                    |
|    |             | <b>F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES</b> |
|    |             | <b><i>Regulation and Supervision</i></b>   |
| 26 | R.23        | Regulation and supervision of financial institutions *   |
| 27 | R.29        | Powers of supervisors  |
| 28 | R.24        | Regulation and supervision of DNFBPs *   |
|    |             | <b><i>Operational and Law Enforcement</i></b>  |
| 29 | R.26        | Financial intelligence units *   |
| 30 | R.27        | Responsibilities of law enforcement and investigative authorities *                              |
| 31 | R.28        | Powers of law enforcement and investigative authorities  |
| 32 | SRIX        | Cash couriers *  |
|    |             | <b><i>General Requirements</i></b>   |
| 33 | R.32        | Statistics   |
| 34 | R.25        | Guidance and feedback  |
|    |             | <b><i>Sanctions</i></b>  |
| 35 | R.17        | Sanctions  |
|    |             | <b>G – INTERNATIONAL COOPERATION</b>   |
| 36 | R.35 & SRI  | International instruments  |
| 37 | R.36 & SRV  | Mutual legal assistance  |
| 38 | R.38        | Mutual legal assistance: freezing and confiscation *   |
| 39 | R.39        | Extradition  |

|  |      |  |
|--|------|--|
| <b>40</b>  | R.40 | Other forms of international cooperation * |
| <p><i>1. The 'old number' column refers to the corresponding 2003 FATF Recommendation.</i></p> <p><i>* Recommendations marked with an asterisk have interpretive notes, which should be read in conjunction with the Recommendation.</i></p> <p><i>Version as adopted on 15 February 2012.</i></p> |      |  |



**Appendix 2: Wolfsberg Group Financial Crime Compliance Questionnaire by Citigroup**

**Inc.**

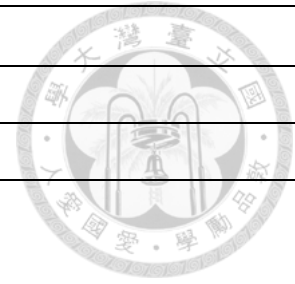


**the  
Wolfsberg  
Group**  
Financial Institution  
Name:  
Location (Country):

|                 |
|-----------------|
| Citigroup, Inc. |
| Global          |

| No #                             | Question  | Answer  |
|----------------------------------|---|---|
| <b>1. ENTITY &amp; OWNERSHIP</b> |   |   |
| 1                                | Full Legal name   | Citigroup, Inc.   |
| 2                                | Append a list of foreign branches which are covered by this questionnaire (if applicable) | This questionnaire is inclusive of Citigroup, Inc. Broker Dealer subsidiaries and branches only. Information regarding any particular Broker Dealer can be made upon request. Additional information can be accessed here:<br><a href="https://www.citigroup.com/citi/investors/pres/html">https://www.citigroup.com/citi/investors/pres/html</a> |
| 3                                | Full Legal (Registered) Address   | 1209 Orange Street, Wilmington, DE 19801  |
| 4                                | Full Primary Business Address (if different from above)                                   | 388 Greenwich Street, New York, NY 10013  |
| 5                                | Date of Entity incorporation / establishment  | March 8, 1988   |
| 6                                | Select type of ownership and append an ownership chart if available                       |   |
| 6 a                              | Publicly Traded (25% of shares publicly traded)   | Yes   |

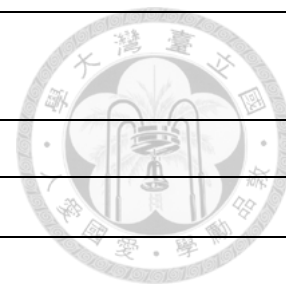
|  |  |  |
|--|--|--|
| <b>6 a1</b>                                  | If Y, indicate the exchange traded on and ticker symbol  | New York Stock Exchange (NYSE) under ticker symbol "C" |
| <b>6 b</b>                                   | Member Owned / Mutual  | No   |
| <b>6 c</b>                                   | Government or State Owned by 25% or more   | No   |
| <b>6 d</b>                                   | Privately Owned  | No   |
| <b>6 d1</b>                                  | If Y, provide details of shareholders or ultimate beneficial owners with a holding of 10% or more                        | N/A  |
| <b>7</b>                                     | % of the Entity's total shares composed of bearer shares   | 0%   |
| <b>8</b>                                     | Does the Entity, or any of its branches, operate under an Offshore Banking License (OBL) ?                               | No   |
| <b>8 a</b>                                   | If Y, provide the name of the relevant branch/es which operate under an OBL  | N/A  |
| <b>2. AML, CTF &amp; SANCTIONS PROGRAMME</b> |  |  |
| <b>9</b>                                     | Does the Entity have a programmed that sets minimum AML, CTF and Sanctions standards regarding the following components: |  |
| <b>9 a</b>                                   | Appointed Officer with sufficient experience / expertise   | Yes  |
| <b>9 b</b>                                   | Cash Reporting   | Yes  |
| <b>9 c</b>                                   | CDD  | Yes  |
| <b>9 d</b>                                   | EDD  | Yes  |
| <b>9 e</b>                                   | Beneficial Ownership   | Yes  |
| <b>9 f</b>                                   | Independent Testing  | Yes  |
| <b>9 g</b>                                   | Periodic Review  | Yes  |
| <b>9 h</b>                                   | Policies and Procedures  | Yes  |
| <b>9 i</b>                                   | Risk Assessment  | Yes  |
| <b>9 j</b>                                   | Sanctions  | Yes  |
| <b>9 k</b>                                   | PEP Screening  | Yes  |
| <b>9 l</b>                                   | Adverse Information Screening  | Yes  |



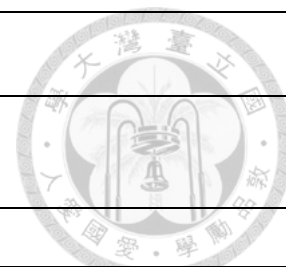
|  |  |  |
|--|--|--|
| <b>9 m</b>   | Suspicious Activity Reporting  | Yes  |
| <b>9 n</b>   | Training and Education   | Yes  |
| <b>9 o</b>   | Transaction Monitoring   | Yes  |
| <b>10</b>  | Is the Entity's AML, CTF & Sanctions policy approved at least annually by the Board or equivalent Senior Management Committee?   | Yes  |
| <b>11</b>  | Does the Entity use third parties to carry out any components of its AML, CTF & Sanctions programmed?  | Yes  |
| <b>11a</b>   | If Y, provide further details  | Citi may contract third parties to perform AML controls. |
| <b>3. ANTI BRIBERY &amp; CORRUPTION</b>                      |  |  |
| <b>12</b>  | Has the Entity documented policies and procedures consistent with applicable ABC regulations and requirements to [reasonably] prevent, detect and report bribery and corruption? | Yes  |
| <b>13</b>  | Does the Entity's internal audit function or other independent third-party cover ABC Policies and Procedures?  | Yes  |
| <b>14</b>  | Does the Entity provide mandatory ABC training to:   |  |
| <b>14 a</b>  | Board and Senior Committee Management  | Yes  |
| <b>14 b</b>  | 1st Line of Defense  | Yes  |
| <b>14 c</b>  | 2nd Line of Defense  | Yes  |
| <b>14 d</b>  | 3rd Line of Defense  | Yes  |
| <b>14 e</b>  | 3rd parties to which specific compliance activities subject to ABC risk have been outsourced   | Yes  |
| <b>14 f</b>  | Non-employed workers as appropriate (contractors / consultants)  | Yes  |
| <b>4. AML, CTF &amp; SANCTIONS POLICIES &amp; PROCEDURES</b> |  |  |
| <b>15</b>  | Has the Entity documented policies and procedures consistent with applicable AML, CTF & Sanctions  |  |



|             |   |     |
|-------------|---|-----|
|             | regulations and requirements to reasonably prevent, detect and report:  |     |
| <b>15 a</b> | Money laundering  | Yes |
| <b>15 b</b> | Terrorist financing   | Yes |
| <b>15 c</b> | Sanctions violations  | Yes |
| <b>16</b>   | Does the Entity have policies and procedures that:  |     |
| <b>16 a</b> | Prohibit the opening and keeping of anonymous and fictitious named accounts   | Yes |
| <b>16 b</b> | Prohibit the opening and keeping of accounts for unlicensed banks and / or NBFIs  | Yes |
| <b>16 c</b> | Prohibit dealing with other entities that provide banking services to unlicensed banks  | Yes |
| <b>16 d</b> | Prohibit accounts / relationships with shell banks  | Yes |
| <b>16 e</b> | Prohibit dealing with another Entity that provides services to shell banks  | Yes |
| <b>16 f</b> | Prohibit opening and keeping of accounts for Section 311 designated entities  | Yes |
| <b>16 g</b> | Prohibit opening and keeping of accounts for any of unlicensed / unregulated remittance agents, exchanges houses, casa de Cambio, bureau de change or money transfer agents | Yes |
| <b>16 h</b> | Assess the risks of relationships with domestic and foreign PEPs, including their family and close associates   | Yes |
| <b>16 i</b> | Define escalation processes for financial crime risk issues   | Yes |
| <b>16 j</b> | Specify how potentially suspicious activity identified by employees is to be escalated and investigated   | Yes |
| <b>16 k</b> | Outline the processes regarding screening for sanctions, PEPs and negative media  | Yes |
| <b>17</b>   | Has the Entity defined a risk tolerance statement or similar document which   | Yes |




|                            |  |  |
|----------------------------|--|--|
|                            | defines a risk boundary around their business?   |  |
| <b>18</b>                  | Does the Entity have a record retention procedure that comply with applicable laws?  | Yes  |
| <b>18 a</b>                | If Y, what is the retention period?  | 5 years or more  |
| <b>5. KYC, CDD and EDD</b> |  |  |
| <b>19</b>                  | Does the Entity verify the identity of the customer?   | Yes  |
| <b>20</b>                  | Do the Entity's policies and procedures set out when CDD must be completed, e.g. at the time of onboarding or within 30 days | Yes  |
| <b>21</b>                  | Which of the following does the Entity gather and retain when conducting CDD?<br>Select all that apply:                      |  |
| <b>21 a</b>                | Ownership structure  | Yes  |
| <b>21 b</b>                | Customer identification  | Yes  |
| <b>21 c</b>                | Expected activity  | Yes  |
| <b>21 d</b>                | Nature of business / employment  | Yes  |
| <b>21 e</b>                | Product usage  | Yes  |
| <b>21 f</b>                | Purpose and nature of relationship   | Yes  |
| <b>21 g</b>                | Source of funds  | Yes  |
| <b>21 h</b>                | Source of wealth   | Yes  |
| <b>22</b>                  | Are each of the following identified:  |  |
| <b>22 a</b>                | Ultimate beneficial ownership  | Yes  |
| <b>22 a1</b>               | Are ultimate beneficial owners verified?   | Yes  |
| <b>22 b</b>                | Authorized signatories (where applicable)  | Yes  |
| <b>22 c</b>                | Key controllers  | Yes  |
| <b>22 d</b>                | Other relevant parties   | Depending on local regulation in countries where Citi has accounts established, the identification of additional relevant parties may be needed. |
| <b>23</b>                  | Does the due diligence process result in customers receiving a risk classification?  | Yes  |



|              |  |  |
|--------------|--|--|
| <b>24</b>    | Does the Entity have a risk-based approach to screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?   | Yes  |
| <b>25</b>    | Does the Entity have policies, procedures and processes to review and escalate potential matches from screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs? | Yes  |
| <b>26</b>    | Does the Entity have a process to review and update customer information based on:   |  |
| <b>26 a</b>  | KYC renewal  | Yes  |
| <b>26 b</b>  | Trigger event  | Yes  |
| <b>27</b>    | From the list below, which categories of customers or industries are subject to EDD and / or are restricted, or prohibited by the Entity's FCC programmed?   |  |
| <b>27 a</b>  | Non-account customers  | Not EDD, not restricted or not prohibited on a risk-based approach |
| <b>27 b</b>  | Non-resident customers   | EDD & restricted on a risk-based approach                          |
| <b>27 c</b>  | Shell banks  | Prohibited   |
| <b>27 d</b>  | MVTS/ MSB customers  | EDD on a risk-based approach                                       |
| <b>27 e</b>  | PEPs   | EDD on a risk-based approach                                       |
| <b>27 f</b>  | PEP Related  | EDD on a risk-based approach                                       |
| <b>27 g</b>  | PEP Close Associate  | EDD on a risk-based approach                                       |
| <b>27 h</b>  | Correspondent Banks  | EDD on a risk-based approach                                       |
| <b>27 h1</b> | If EDD or EDD & restricted, does the EDD assessment contain the elements as set out in the Wolfsberg Correspondent Banking Principles 2014?  | Yes  |
| <b>27 i</b>  | Arms, defense, military  | EDD & restricted on a risk-based approach                          |
| <b>27 j</b>  | Atomic power   | EDD & restricted on a risk-based approach                          |
| <b>27 k</b>  | Extractive industries  | EDD on a risk-based approach                                       |
| <b>27 l</b>  | Precious metals and stones   | EDD & restricted on a risk-based approach                          |



|                                      |   |   |
|--------------------------------------|---|---|
| <b>27 m</b>                          | Unregulated charities   | EDD on a risk-based approach  |
| <b>27 n</b>                          | Regulated charities   | EDD on a risk-based approach  |
| <b>27 o</b>                          | Red light business / Adult entertainment  | EDD & restricted on a risk-based approach                                     |
| <b>27 p</b>                          | Non-Government Organizations  | EDD on a risk-based approach  |
| <b>27 q</b>                          | Virtual currencies  | Prohibited  |
| <b>27 r</b>                          | Marijuana   | EDD & restricted on a risk-based approach                                     |
| <b>27 s</b>                          | Embassies / Consulates  | EDD on a risk-based approach  |
| <b>27 t</b>                          | Gambling  | EDD on a risk-based approach  |
| <b>27 u</b>                          | Payment Service Provider  | EDD on a risk-based approach  |
| <b>27 v</b>                          | Other (specify)   | N/A   |
| <b>28</b>                            | If restricted, provide details of the restriction   | EDD and restrictions will vary by jurisdiction in accordance with local laws. |
| <b>6. MONITORING &amp; REPORTING</b> |   |   |
| <b>29</b>                            | Does the Entity have risk-based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?                | Yes   |
| <b>30</b>                            | What is the method used by the Entity to monitor transactions for suspicious activities?  | Combination of automated and manual   |
| <b>31</b>                            | Does the Entity have regulatory requirements to report suspicious transactions?   | Yes   |
| <b>31 a</b>                          | If Y, does the Entity have policies, procedures and processes to comply with suspicious transactions reporting requirements?                              | Yes   |
| <b>32</b>                            | Does the Entity have policies, procedures and processes to review and escalate matters arising from the monitoring of customer transactions and activity? | Yes   |
| <b>7. PAYMENT TRANSPARENCY</b>       |   |   |
| <b>33</b>                            | Does the Entity adhere to the Wolfsberg Group Payment Transparency Standards?   | Yes   |

|                     |  |  |
|---------------------|--|--|
| <b>34</b>           | Does the Entity have policies, procedures and processes to [reasonably] comply with and have controls in place to ensure compliance with:  |                               |
| <b>34 a</b>         | FATF Recommendation 16   | Yes  |
| <b>34 b</b>         | Local Regulations  | Yes  |
| <b>34 b1</b>        | Specify the regulation   | In jurisdictions where Citi operates, it has policies and procedures to comply with applicable local regulation. |
| <b>34 c</b>         | If N, explain  | N/A  |
| <b>8. SANCTIONS</b> |  |  |
| <b>35</b>           | Does the Entity have policies, procedures or other controls reasonably designed to prohibit and / or detect actions taken to evade applicable sanctions prohibitions, such as stripping, or the resubmission and / or masking, of sanctions relevant information in cross border transactions? | Yes  |
| <b>36</b>           | Does the Entity screen its customers, including beneficial ownership information collected by the Entity, during onboarding and regularly thereafter against Sanctions Lists?  | Yes  |
| <b>37</b>           | Select the Sanctions Lists used by the Entity in its sanctions screening processes:  |  |
| <b>37 a</b>         | Consolidated United Nations Security Council Sanctions List (UN)   | Used for screening customers and beneficial owners and for filtering transactional data                          |
| <b>37 b</b>         | United States Department of the Treasury's Office of Foreign Assets Control (OFAC)   | Used for screening customers and beneficial owners and for filtering transactional data                          |
| <b>37 c</b>         | Office of Financial Sanctions Implementation HMT (OFSI)  | Used for screening customers and beneficial owners and for filtering transactional data                          |
| <b>37 d</b>         | European Union Consolidated List (EU)  | Used for screening customers and beneficial owners and for filtering transactional data                          |
| <b>37 e</b>         | Lists maintained by other G7 member countries  | Used for screening customers and beneficial owners and for filtering transactional data                          |

|                                    |  |  |
|------------------------------------|--|--|
| 37 f                               | Other (specify)  | Citi screens against the lists issued and jurisdictions subject to sanctions pursuant to local sanctions laws and regulations (non-U.S. Sanctions) in each jurisdiction where it conducts business |
| 38                                 | Does the Entity have a physical presence, e.g., branches, subsidiaries, or representative offices located in countries / regions against which UN, OFAC, OFSI, EU and G7 member countries have enacted comprehensive jurisdiction-based Sanctions? | No   |
| <b>9. TRAINING &amp; EDUCATION</b> |  |  |
| 39                                 | Does the Entity provide mandatory training, which includes:  |  |
| 39 a                               | Identification and reporting of transactions to government authorities   | Yes  |
| 39 b                               | Examples of different forms of money laundering, terrorist financing and sanctions violations relevant for the types of products and services offered  | Yes  |
| 39 c                               | Internal policies for controlling money laundering, terrorist financing and sanctions violations   | Yes  |
| 39 d                               | New issues that occur in the market, e.g., significant regulatory actions or new regulations   | Yes  |
| 40                                 | Is the above mandatory training provided to :  |  |
| 40 a                               | Board and Senior Committee Management  | Yes  |
| 40 b                               | 1st Line of Defense  | Yes  |
| 40 c                               | 2nd Line of Defense  | Yes  |
| 40 d                               | 3rd Line of Defense  | Yes  |
| 40 e                               | 3rd parties to which specific FCC activities have been outsourced  | Yes  |
| 40 f                               | Non-employed workers (contractors / consultants)   | Yes  |
| <b>10. AUDIT</b>                   |  |  |
| 41                                 | In addition to inspections by the government supervisors/regulators, does the Entity have an internal audit function, a testing function, or another independent third party, or both, that  | Yes  |

assesses FCC AML, CTF and Sanctions policies and practices on a regular basis?



**Signature Page**

“Wolfsberg Group Financial Crime Compliance Questionnaire” 2020 (FCCQ V1.1)

I certify that I have read and understood this declaration, that the answers provided in this Wolfsberg FCCQ are complete and correct to my honest belief.

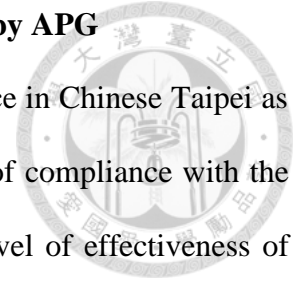
Financial Institution name: Citigroup, Inc.

Senior Compliance Manager- Second Line representative: Jacqueline Sanjuas

A handwritten signature in cursive script, appearing to read "Jacqueline Sanjuas".

Date: 5/25/2021  
(Signature & Date)

### Appendix 3: Chinese Taipei Mutual Evaluation Report by APG



This report provides a summary of the AML/CFT measures in place in Chinese Taipei as at the end of the on-site visit (16 November 2018). It analyses the level of compliance with the “Financial Action Task Force” (FATF) 40 Recommendations and the level of effectiveness of Chinese Taipei’s AML/CFT system, and provides recommendations on how the system could be strengthened.

1. Chinese Taipei has pursued wide ranging reforms since early 2017, with very significant progress achieved in a short period of time. This reflects strong political commitment to AML/CFT reform, significant commitment of resources, effective coordination, and efforts to strengthen and deepen the culture and practice of money laundering / terrorist financing (ML/TF) risk management.
2. Chinese Taipei has a generally sound understanding of its ML/TF risks which is reflected in its public national risk assessment (NRA) and other assessments. National and agency-level AML/CFT policies and activities seek to address the risks identified in the assessments. Co- ordination and co-operation on AML/CFT issues at both the policy and operational levels has improved significantly since the last evaluation.
3. Financial intelligence and related information is used extensively in ML and predicate offence investigations and in tracing criminal proceeds. Law enforcement agencies (LEAs) are well- equipped and experienced in generating and using financial intelligence to follow money trails and uncover complex structures and networks. The Anti-Money Laundering Division of the MJIB (AML D) - Chinese Taipei’s financial intelligence unit (FIU) - produces good quality intelligence and adds value in financial investigations, particularly those involving international elements.



4. Law enforcement agencies (LEAs), including prosecutors, conduct complex ML investigations actively tracing money trails, lifting the corporate veil, unravelling layers of ownership and pursuing funds sent offshore. Prosecutors drive ML investigations and coordinate authorities according to expertise. The range of ML investigations and prosecutions is generally in line with the risk profile with the exception of relatively low numbers of ML related to drug trafficking and smuggling. However, authorities are not using the ML offence to the extent necessary across a broad range of conduct in the context of Chinese Taipei. The conviction rate for ML is low and the penalties applied have not been dissuasive. Chinese Taipei has used a variety of tools in identifying, tracing and forfeiting criminal assets which operate well in practice. Chinese Taipei is successful in forfeiting a significant value of assets when compared to the size of its economy. Forfeiture appears to be consistent with Chinese Taipei's risk profile.
5. A number of financial investigations of suspected TF cases have been successfully undertaken. They involved intelligence sharing and ultimately uncovered conduct that was unrelated to TF. There have been no TF convictions, which is in keeping with Chinese Taipei's TF risk profile.
6. Chinese Taipei has strong policy and operational coordination mechanisms to support the implementation of targeted financial sanctions (TFS) to combat terrorism and proliferation of weapons of mass destruction (WMD). Authorities have issued guidance to all sectors and undertaken a great deal of outreach to all financial institutions (FI) and designated non- financial businesses and professions (DNFBP) sectors and have supported all sectors to have access to screening software to support implementation of TFS. FIs, especially banks, demonstrate a good understanding of TFS obligations and

the implementation of customer and transaction monitoring to identify possible sanctions matches.

7. Implementation of TFS for DPRK-related designations has resulted in 81 freezing actions worth over USD 3.96 million. While there are minor shortcomings in the scope of TFS for proliferation financing (PF), the legal framework goes beyond FATF standards by also establishing a PF offence, related suspicious transaction reporting (STR) obligations and a domestic designation system for TFS. Chinese Taipei has designated a local and entities working on his behalf/at his direction linked to PF and subjected them to TFS, resulting in freezing considerable assets. A large number of PF-related STRs have been received and intelligence has been developed to identify possible networks of associates. Authorities have granted access to frozen funds for basic expenses in keeping with the standards.
8. Technical compliance elements for preventive measures are generally comprehensive. There has been a shift towards a risk-based approach in the banking sector since 2013, but this approach is newer in many other sectors. Sectoral supervisors have undertaken very significant amounts of awareness raising on AML/CFT obligations and ML/TF risks. Tailored guidance has been issued for each sector.
9. Chinese Taipei has a generally robust system of AML/CFT supervision for FIs. AML/CFT supervision of DNFBP sectors has only recently commenced. The sanctions imposed on banks, securities and insurance for AML/CFT breaches are relatively low and may not be wholly effective or proportionate. More broadly than the level of fines, overall the effects of supervisory actions have significantly influenced compliance in a positive way through remedial measures, enforcement actions and reputation damage.

10. Authorities have a mixed understanding of the risks associated with legal persons and legal arrangements. Authorities rely on CDD conducted by FIs and DNFBPs to obtain up to date beneficial ownership information of legal persons and arrangements. LEAs and the AMLD demonstrated examples of using CDD information and investigative strategies to obtain information on the beneficial ownership and control of legal persons. The scope and quality of the information held on the company registry has greatly improved in the period prior to this assessment. There are a number of controls on legal persons to mitigate their risk of misuse related to nominee shares and nominee directors. Despite the large numbers of civil trusts formed in Chinese Taipei, there are few measures to support the transparency of trusts and capturing information on settlors or trustees.
11. Chinese Taipei provides good quality constructive assistance for international cooperation requests related to ML and asset restraint and forfeiture.