

2024

National Money Laundering, Terrorist
Financing and Proliferation Financing
Risk Assessment Report



行政院洗錢防制辦公室
Anti-Money Laundering Office, Executive Yuan

Preface

As a founding member of the Asia–Pacific Group (APG) on Money Laundering, Taiwan has consistently upheld a strong sense of responsibility and has been actively engaged in AML, CFT, and CPF. In addition to continuously complying with the latest recommendations issued by the Financial Action Task Force (FATF), we have demonstrated the government’s firm resolve to counter ML/FT/PF through interagency collaboration and public–private partnerships.

In 2019, Taiwan was placed in “regular follow-up”, the most favorable follow-up category under the third round of APG mutual evaluations, but our efforts have remained unwavering. Based on these foundations, this National Risk Assessment (NRA) report not only builds on our previous achievements but, for the first time, also includes “foreign migrant worker remittance companies” within the scope of assessment and refines the evaluation criteria for certain sectors to more effectively examine the risks faced by Taiwan. Additionally, 53 public sector agencies and 23 private sector organizations were invited to participate, with the hope that their expertise will help foster collective intelligence and deepen national risk identification and mitigation strategies.

The Executive Yuan places great emphasis on the “Five Crackdowns and Seven Safeguards” policy, prioritizing the fight against organized crime, illicit finance, firearms, narcotics, and fraud, with AML efforts closely intertwined with these priorities. This is because after committing crimes, perpetrators often employ various means to conceal and disguise their illicit proceeds, thereby hindering law enforcement investigations and ultimately benefiting from these illegal gains. Strengthening AML measures enables us to more effectively combat such criminal activities.

However, with advancements in technology, criminal methods continue to evolve, and existing measures may be insufficient. As the saying goes, “When circumstances reach an impasse, one must change; through change, a way forward opens.” We have adopted the “ABC” strategy to update and strengthen Taiwan’s AML/CFT/CPF efforts in response to the challenges presented by emerging technologies.

“A” stands for “Adaptation”: recently, the government has comprehensively amended and introduced new special laws—including the Money Laundering Control Act and the Fraud Crime Hazard Prevention Act—as part of the “Four New Anti-Fraud Laws,” thereby enhancing law enforcement tools to bring offenders to justice. “B” stands for “Block”: when confronted with new types of fraud, we have adopted advanced digital tools, enhanced public outreach campaigns on fraud identification, and at the same time strengthened the supervision of virtual asset service providers. “C” stands for “Cooperation”: through close collaboration with countries worldwide and international organizations such as the APG, we ensure that transnational crime has nowhere to hide.

Looking ahead, we will use the findings of this NRA as a key reference for policy development and implementation, safeguarding the transparency and order of the financial environment. We are committed to ensuring that Taiwan continues to play a pivotal role in AML/CFT/CPF efforts in the Asia-Pacific region and globally, setting a benchmark in combating money laundering, terrorist financing, and proliferation financing.

Premier, Executive Yuan



December 6, 2024



CONTENTS

2024 National ML/FT/PF Risk Assessment Report

| | |
|---|----|
| Chapter 1. Introduction | 1 |
| Chapter 2. Legal Framework and Organizational Structure | 4 |
| Section 1. Taiwan's Legal Framework for AML/CFT/CPF | 4 |
| Section 2. Competent Authorities for AML/CFT/CPF in Taiwan | 5 |
| Chapter 3. Risk Assessment Procedures and Methodology | 7 |
| Section 1. Risk Assessment Procedures | 7 |
| Section 2. Risk Assessment Methodology | 9 |
| Chapter 4. Overview of Risk Assessment Results | 13 |
| Section 1. Money Laundering Risk | 13 |
| Section 2. Terrorist Financing Risk | 14 |
| Section 3. Proliferation Financing Risk | 14 |
| Chapter 5. Risk Assessment Results: Money Laundering and Terrorist Financing Threats | 15 |
| Section 1. Money Laundering Threats | 15 |
| Section 2. Terrorism Financing Threats | 32 |
| Chapter 6. Risk Assessment Results: Money Laundering and Terrorist Financing Vulnerabilities | 34 |
| Section 1. National Assessment Results for ML/FT Vulnerabilities | 34 |
| Section 2. Assessment Results of the Industry/Sector ML/FT Vulnerabilities | 43 |
| Chapter 7. Risk Assessment Results: Proliferation Financing Risk | 73 |
| Section 1. Proliferation Financing Threats | 73 |
| Section 2. Vulnerabilities in Proliferation Financing | 75 |
| Section 3. Proliferation Financing Risk Assessment Results | 81 |
| Chapter 8. Risk Assessment Results: Legal Persons | 82 |

| | |
|---|-----|
| Chapter 9. Risk Assessment Results: Legal Arrangements/Trusts..... | 89 |
| Chapter 10. Risk Assessment Results: Non-Profit Organizations | 94 |
| Section 1. Higher-Risk Non-Profit Organizations | 94 |
| Section 2. Lower-Risk Non-Profit Organizations..... | 96 |
| Chapter 11. National Strategy and Future Plans | 99 |
| Annex 1: Taiwan’s Legal Framework for AML/CFT/CPF ... | 102 |
| Annex 2: Competent Authorities for AML/CFT/CPF in Taiwan | 108 |
| Annex 3: Factors and Classification Definitions for Money Laundering Threat Analysis | 114 |
| Annex 4: Factors and Classification Definitions for Terrorist Financing Threat Analysis | 116 |
| Annex 5: Factors and Classification Definitions for Money Laundering and Terrorist Financing Vulnerability Analysis | 118 |
| Annex 6: Factors and Classification Definitions for Proliferation Financing Threat Analysis..... | 123 |
| Annex 7: Factors and Classification Definitions for Proliferation Financing Vulnerability Analysis..... | 124 |
| Appendix: Meeting Minutes Compilation..... | 129 |

Chapter 1. Introduction

The Asia/Pacific Group on Money Laundering (APG) initiated the third round of mutual evaluations on Taiwan in November 2018. On June 28, 2019, its preliminary report was officially released, with Taiwan placed in the highest “regular follow-up” category. This achievement was adopted at the APG annual meeting in Canberra, Australia, in August of the same year, and the results were subsequently announced on October 2 following the completion of the global mutual evaluation review. Taiwan achieved the best results among APG member jurisdictions in the Asia–Pacific region, clearly demonstrating that the joint efforts of the government and civil society to combat money laundering (ML) have been widely recognized and affirmed internationally.

The Basel Institute on Governance released the “Basel AML Index 2023¹” in November 2023, ranking Taiwan 133rd out of 152 jurisdictions worldwide for ML risk, with only New Zealand and Australia performing better in the Asia–Pacific region. Additionally, the Institute for Economics and Peace published the “Global Terrorism Index 2024²”, in which Taiwan ranked 89th, indicating a low risk of money laundering (ML) and financing of terrorism (FT).

To strengthen AML/CFT efforts, Taiwan established the Anti-Money Laundering Office, Executive Yuan, in 2017. Between 2017 and 2018, Taiwan conducted its first national assessment of predicate crime threats and sectoral vulnerabilities related to ML/FT risks. This assessment enabled both the public and private sectors to gain a clearer understanding of Taiwan’s risk landscape. Based on the findings, appropriate risk-mitigation measures were implemented to address the most significant threats and vulnerabilities, and both the national and sectoral AML/CFT frameworks were further aligned with international standards.

Subsequently, in 2021, Taiwan conducted its second National ML/FT Risk Assessment. This assessment involved a greater number of participating agencies and personnel, strengthened domestic and international data collection, and, for the first time, incorporated an assessment of proliferation financing (PF) risk. The assessment methodology partially drew from approaches developed by the Royal United Services Institute (RUSI)³, adapted to Taiwan’s specific context. In response to evolving criminal threats and the latest domestic and international risk trends, “illegal gambling (including online gambling)” was added to the threat risk assessment. To enable a more detailed review, “underground banking” was assessed separately from “third-party money laundering.” For the vulnerability assessment, new sectors such as “virtual asset service providers,” “online gaming businesses,” “art auction houses,” “automobile trading (including used cars),” and “pawnshops” were included for the first time.

¹ Source: <https://baselgovernance.org/sites/default/files/2023-11/Basel%20AML%20Index%202023%2012th%20Edition.pdf> (Last accessed: November 12, 2024).

² Source: <https://www.visionofhumanity.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf> (Last accessed: November 12, 2024).

³ Source: https://static.rusi.org/20190513_guide_to_conducting_a_national_proliferation_financing_risk_assessment_web.pdf (Last accessed: November 12, 2024).

In 2024, Taiwan conducted its third National ML/FT/PF Risk Assessment. Building on past experience, a total of 53 public sector agencies⁴ and 23 private sector associations and organizations⁵ participated. During the assessment period, input from both domestic and international experts and scholars was sought to provide a comprehensive, multifaceted view of Taiwan's current risk landscape.

In addition, with regard to industry/sector ML/FT vulnerabilities, and in response to the December 2021 amendments to Taiwan's Regulations Governing Anti-Money Laundering of Financial Institutions, foreign migrant worker remittance companies have been included within the definition of financial institutions under these Regulations. Accordingly, foreign migrant worker remittance companies are also included within the scope of this risk assessment. Taking industry practices into consideration and to facilitate the effective allocation of supervisory resources, certain sectoral assessment categories have been adjusted. "Futures trust enterprises" have been incorporated into the consolidated assessment of "securities investment trust enterprises," now referred to as "securities investment trust enterprises (including futures trust enterprises)." Similarly, "managed futures enterprises" and "leverage transaction merchants" have been merged into the category of "futures commission merchants (including managed futures enterprises and leverage transaction merchants)". In line with the latest amendments to the Money Laundering Control Act promulgated on July 31, 2024, the sector previously referred to as the "virtual asset industry" has been revised to "enterprise or person providing virtual asset services (virtual asset service providers)" and "third-party payment service

⁴ Public sector agencies include the following: National Security Bureau; Civil Department, Judicial Yuan; Criminal Department, Judicial Yuan; Ministry of Foreign Affairs; Ministry of National Defense; Ministry of Education; Ministry of Justice; Ministry of Economic Affairs; Ministry of Labor; Ministry of Agriculture; Ministry of Environment; Ministry of Culture; Mainland Affairs Council; Financial Supervisory Commission; Public Construction Commission, Executive Yuan; Central Bank; Taiwan High Prosecutors Office; Taipei District Prosecutors Office, Taiwan; Department of Cooperatives and Civil Associations, Ministry of the Interior; Department of Land Administration, Ministry of the Interior; Department of Religious Affairs and Rites, Ministry of the Interior; National Immigration Agency, Ministry of the Interior; National Police Agency, Ministry of the Interior; Department of International Fiscal Affairs, Ministry of Finance; National Treasury Administration, Ministry of Finance; Taxation Administration, Ministry of Finance; Customs Administration, Ministry of Finance; Department of Prosecutorial Affairs, Ministry of Justice; Department of Legal Affairs, Ministry of Justice; Department of International and Cross-Strait Legal Affairs, Ministry of Justice; Investigation Bureau, Ministry of Justice; Agency Against Corruption, Ministry of Justice; Administrative Enforcement Agency, Ministry of Justice; Department of Commerce, Ministry of Economic Affairs; Bureau of Foreign Trade, Ministry of Economic Affairs; Bureau of Energy, Ministry of Economic Affairs; Intellectual Property Office, Ministry of Economic Affairs; Maritime and Port Bureau, Ministry of Transportation and Communications; Agricultural Finance Agency, Ministry of Agriculture; Fisheries Agency, Ministry of Agriculture; Department of Medical Affairs, Ministry of Health and Welfare; Department of Social and Family Affairs, Ministry of Health and Welfare; Food and Drug Administration, Ministry of Health and Welfare; Resource Circulation Administration, Ministry of Environment; Administration for Cyber Security, Ministry of Digital Affairs; Administration for Digital Industries, Ministry of Digital Affairs; Banking Bureau, Financial Supervisory Commission; Insurance Bureau, Financial Supervisory Commission; Securities and Futures Bureau, Financial Supervisory Commission; Examination Bureau, Financial Supervisory Commission; Coast Guard Administration, Ocean Affairs Council; Office of Homeland Security, Executive Yuan; Anti-Money Laundering Office, Executive Yuan; etc.

⁵ Private sector associations include the following: Taiwan Stock Exchange Corporation, Taiwan Futures Exchange Corporation, Taiwan Depository & Clearing Corporation, Taipei Exchange (TPEX), The Bankers Association of the Republic of China, The National Federation of Credit Cooperatives, Trust Association of the Republic of China, Bills Finance Association of the Republic of China, Life Insurance Association of the Republic of China, Non-Life Insurance Association of the Republic of China, Insurance Brokers Association of the Republic of China, Insurance Agents Association of the Republic of China, Securities Association of the Republic of China, Securities Investment Trust & Consulting Association of the Republic of China, Futures Association of the Republic of China, National Bar Association, National Federation of Certified Public Accountants Associations of the Republic of China, National Association of Real Estate Brokers, National Association of Land Administration Agents, National Association of Bookkeepers, National Association of Bookkeeping and Tax Agents, National Jewelry & Gold Merchants Association of the Republic of China, and the National Association of Non-Store Retailers

industry” has been revised to “enterprises or persons providing third-party payment services (third-party payment service providers)”. Additionally, in response to the revisions of Recommendations 24 and 25 of the Financial Action Task Force (FATF), “foreign legal persons” and “foreign legal arrangements/trusts” have been included in the scope of the risk assessment for the first time.

Through this comprehensive and in-depth review, Taiwan has established a solid foundation for addressing future risks of ML, FT, and PF, thereby contributing to a more stable and healthy development environment for domestic industries. At the same time, we will continue to align with international standards and fulfill our global responsibilities with an international perspective. Upon completion of the NRA, all public sector agencies are required to review the rationality of their internal policies, regulations, and resource allocation while also assisting the private sector in implementing relevant preventive measures. These combined efforts will further reinforce Taiwan’s overall AML/CFT/CPF framework and support the achievement of outstanding results in the upcoming fourth round of APG mutual evaluations.

Chapter 2. Legal Framework and Organizational Structure

As a founding member of the Asia/Pacific Group on Money Laundering (APG), the government has been dedicated to establishing a robust anti-money laundering (AML) regime by continuously optimizing relevant legal frameworks and financial supervisory measures. By establishing legal systems, Taiwan has built a sound financial environment with transparent financial flows. Furthermore, driven by comprehensive government policy initiatives, the scope of agencies involved in AML, CFT, and CPF is extensive, encompassing nearly all administrative and judicial authorities. A description of Taiwan's relevant legal framework and the organizational structure of competent authorities for implementing AML, CFT, and CPF measures is provided as follows:

Section 1. Taiwan's Legal Framework for AML/CFT/CPF

The legal framework for AML, CFT, and CPF measures is centered on two core statutes: the Money Laundering Control Act and the Counter-Terrorism Financing Act. Each administrative agency is tasked with formulating relevant AML/CFT/CPF regulations and administrative orders within its area of responsibility to ensure compliance with international standards. The Money Laundering Control Act aims to prevent ML, combat crime, establish a robust AML regime, maintain financial order, promote transparency of financial flows, and strengthen international cooperation. The Counter-Terrorism Financing Act was enacted to prevent and suppress the provision of funds to terrorist activities, organizations, and individuals; safeguard national security; protect fundamental human rights; and enhance international cooperation. As AML/CFT/CPF are important policy objectives for the government, the relevant laws and regulations are regularly updated. A summary of the Money Laundering Control Act and Counter-Terrorism Financing Act is provided below, while other related key regulations are listed in Annex 1.

1. Money Laundering Control Act

Enacted in 1996, the Money Laundering Control Act is among the earliest dedicated AML statutes in Asia. It has since undergone multiple amendments, with a primary focus on investigating and prosecuting major crimes. In 2016, the Act was substantially amended to comply with the FATF 40 Recommendations, strengthen Taiwan's AML regime, stabilize financial order, and align with international standards. The amendment was promulgated by the President on December 28, 2016, and officially implemented on June 28, 2017, marking the most significant revision since its original enactment in 1996. The 2016 amendment focused on four main aspects: enhancing the prosecutability of ML offenses, strengthening measures for controlling financial flows, improving internal audit and internal control systems, and bolstering international cooperation on AML. Subsequently, owing to gaps in the regulations, recurring practical disputes, and some provisions not aligning with international standards, the Act was further amended slightly and promulgated on November 7, 2018. The key focus of this amendment is the expansion of regulated entities and the scope of sanctions, including bringing enterprises handling virtual currency platform or transaction under the coverage of the Money Laundering Control Act, thereby subjecting them to the provisions of the Act governing financial institutions.

To block and prevent criminal organizations from the mass collection of individuals' financial institution accounts, virtual asset accounts, or third-party payment accounts, the law now prohibits anyone from transferring or providing these accounts to others for use without a legitimate reason. To address the issue of accounts being used as front accounts for criminal organizations, the Money Laundering Control Act was further amended and promulgated on June 14, 2023. This amendment introduced the offense of collecting accounts or account numbers without legitimate reason, explicitly prohibiting anyone from transferring or providing such accounts or numbers to others without a valid purpose.

To address deficiencies identified in Taiwan's AML regime during the third round of APG mutual evaluations and to implement risk-based approaches (RBA), the Money Laundering Control Act was comprehensively revised and promulgated on July 31, 2024. The revisions target common types of ML offenses, emerging criminal typologies, and issues related to the application of the elements constituting ML crimes. This amendment covers the definition of ML, its constituent elements, and penalties for ML offenses. It introduces AML requirements and registration or licensing regimes for virtual asset service providers and third-party payment service providers, as well as criminal penalties for non-compliance. These changes are intended to align the Act with international standards and enhance enforcement efficacy to more effectively combat ML crimes.

2. Counter-Terrorism Financing Act

In 2016, following the Paris terrorist attacks and a global "Terrorist Financing Fact-Finding Exercise" surveying CFT regulations among member countries, it was revealed that Taiwan's Money Laundering Control Act only included provisions related to FT activities. However, it lacked specific offenses addressing funding for terrorists or terrorist organizations, as well as targeted financial sanctions. To address gaps in the legal framework that could hinder Taiwan's ability to respond to international terrorist activities, the Counter-Terrorism Financing Act was officially promulgated and implemented on July 27, 2016. This Act criminalizes the financing of terrorists, terrorist organizations, and terrorist activities and establishes targeted financial sanctions for FT and PF. Subsequently, to promptly and effectively restrict the transfer of assets of designated sanctioned entities, prevent information leaks, and ensure the effective implementation of sanctions and consistency in statutory terminology, relevant provisions were slightly amended, and this revision was officially promulgated on November 7, 2018.

Section 2. Competent Authorities for AML/CFT/CPF in Taiwan

The competent authorities responsible for AML, CFT, and CPF in Taiwan encompass nearly all administrative and judicial agencies. In terms of legal framework and policy, the Ministry of Justice has traditionally served as the lead authority, responsible for enacting the Money Laundering Control Act and the Counter-Terrorism Financing Act and for coordinating relevant ministries and agencies in formulating AML/CFT/CPF policies. In 2016, following a Taiwanese financial institution being sanctioned by an overseas financial regulator, the Anti-Money Laundering Office was formally established under the Executive Yuan in March 2017 to coordinate Taiwan's AML/CFT policies and to ensure resource allocation among relevant agencies, with responsibility for policy planning and oversight.

For preventive measures, the supervision of sectors and personnel of financial and non-financial institutions is assigned to various competent authorities. Financial institutions are supervised by the Financial Supervisory Commission, the Agricultural Finance Agency of the Ministry of Agriculture, and the Central Bank. Designated non-financial businesses and professions (DNFBPs) are overseen by the Department of Prosecutorial Affairs of the Ministry of Justice, the Securities and Futures Bureau of the Financial Supervisory Commission, the Department of Land Administration of the Ministry of the Interior, the Administration of Commerce of the Ministry of Economic Affairs, the Civil Department of the Judicial Yuan, the Taxation Administration of the Ministry of Finance, and the Administration for Digital Industries of the Ministry of Digital Affairs. Central authorities responsible for non-profit organization (NPO) affairs include the Ministry of the Interior, the Ministry of Health and Welfare, the Ministry of Education, and the Ministry of Culture.

Law enforcement agencies include all levels of prosecutors' offices under the Ministry of Justice, the Investigation Bureau of the Ministry of Justice, the Agency Against Corruption of the Ministry of Justice, the Administrative Enforcement Agency of the Ministry of Justice, the Criminal Department of the Judicial Yuan and all levels of courts, the National Police Agency and the National Immigration Agency of the Ministry of the Interior, and the Coast Guard Administration of the Ocean Affairs Council, as well as the AML Division of the Investigation Bureau of the Ministry of Justice, which serves as the Financial Intelligence Unit.

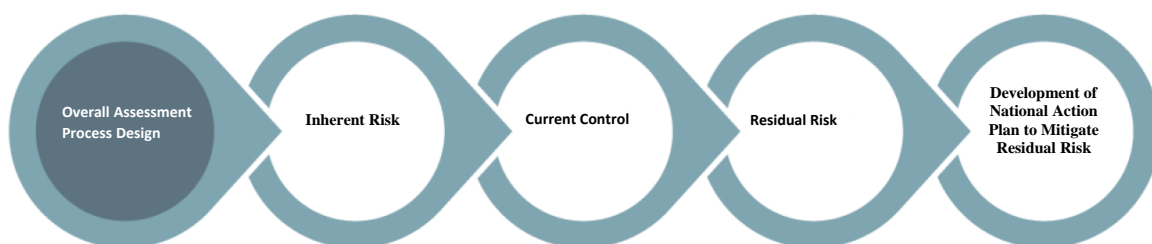
In terms of international cooperation, the Department of International and Cross-Strait Legal Affairs of the Ministry of Justice, the Ministry of Foreign Affairs, the Mainland Affairs Council, and international cooperation units of various ministries and agencies are involved. Additionally, other relevant ministries and agencies participate in issues related to CFT and CPF.

The range of government agencies involved in Taiwan's AML, CFT, and CPF efforts is extensive. To evaluate the adequacy of resources allocated for their responsibilities and policy implementation, the specific mandates and budgets of each relevant agency are detailed in Annex II.

Chapter 3. Risk Assessment Procedures and Methodology

Section 1. Risk Assessment Procedures

In 2017, with the assistance of external consultants, the Anti-Money Laundering Office, Executive Yuan (AMLO), developed national AML/CFT risk assessment procedures and methodologies tailored to the Taiwanese context and the needs of each sector. Subsequent work plans were formulated and formally approved by the Executive Yuan. The procedure consists primarily of the following components: designing the assessment process, conducting inherent risk assessments, analyzing the effectiveness of existing control measures and evaluating residual risk, and developing an action plan to mitigate risks, as detailed in the diagram below.



With the assistance of RUSI in 2021, Taiwan developed an assessment methodology for PF risk tailored to its context; this methodology was incorporated into the overall risk assessment process. It responded to changes in international standards at the time, which required both public and private sectors to identify, assess, understand, and mitigate their PF risks.

Assessment process design is aimed at ensuring that risk assessment information—including the source, nature, and level of each risk—is sufficiently comprehensive to enable relevant authorities to develop appropriate risk mitigation measures. The guiding principles for the risk assessment procedure include the following: assessment objectives, scope, process, assessment phases, participants, users of assessment information and other relevant groups, available information, final outcomes, methods and strategies for dissemination and outreach, and mechanisms for future risk updates. Through this process, “threats” and “vulnerabilities” are identified and assessed to gain a clear understanding of Taiwan’s inherent ML/FT/PF risks. Subsequently, by analyzing the effectiveness of existing control measures, the residual risks are determined. Based on these results, subsequent action plans are formulated, detailing specific risk mitigation measures and their prioritization.

The current ML/FT/PF risk assessment procedure continues to follow this process. With the support of external consultants, a new assessment methodology was introduced for evaluating control measures. By analyzing implementation effectiveness across the public and private sectors from both national and industry/sector perspectives, the methodology enables a more granular examination of residual ML/TF/PF risks, providing a solid foundation for formulating the national strategy and action plan. During this period, the AMLO convened multiple large-scale national risk assessment (NRA) meetings and numerous smaller meetings

involving different agencies, with participants spanning public sector agencies and private sector associations and organizations. A summary of key meeting activities is as follows:

1. On July 22, 2024, the first National ML/FT/PF Risk Assessment Procedure Meeting was held to identify and assess “money laundering threats,” including via both qualitative and quantitative research. Prior to the meeting, each law enforcement agency completed the threat profile form using data drawn from enforcement experience, analytical reports from the Financial Intelligence Unit, and statistics provided by relevant competent authorities. During the meeting, participants reached consensus on the rating of analysis results.
2. On July 29, 2024, the second National ML/FT/PF Risk Assessment Procedure Meeting was held to identify and assess “terrorist financing threats,” “NPO vulnerabilities,” and “proliferation financing risks,” with related content covering both qualitative and quantitative research. Prior to the meetings, each competent authority completed the threat profile form using information drawn from various business information and statistical reports provided by supervisory and law enforcement agencies. During the meeting, participants reached consensus on the rating of analysis results.
3. On July 30, 2024, the third National ML/FT/PF Risk Assessment Procedure Meeting was convened to identify and assess “ML/FT vulnerabilities.” Organizations from both the public and private sectors participated, conducting assessments on “industry/sector,” “legal persons,” and “legal arrangements/trusts.” The assessment incorporated both qualitative and quantitative research. Before the meeting, each supervisory authority completed the analysis table, with information sources including various business information and statistical reports provided by supervisory authorities. During the meeting, participants reached consensus on the rating of analysis results.
4. On August 30 and September 6, 2024, the fourth and fifth National ML/FT/PF Risk Assessment Procedure Meetings were held to identify and assess “control effectiveness and residual risk” and to draft the “National AML/CFT/CPF Strategy” and the “AML/CFT/CPF Action Plan.” The content included both qualitative and quantitative research. Prior to the meetings, each supervisory and law enforcement authority completed the assessment forms evaluating the effectiveness of controls at both the national and industry/sector levels. Information sources included various business information and statistical reports from supervisory and law enforcement agencies. During the meetings, participants reached a consensus on the rating of analysis results.
5. On September 12, 2024, the sixth National ML/FT/PF Risk Assessment Procedure Meeting was held to review and approve the “National AML/CFT/CPF Strategy” and the “AML/CFT/CPF Action Plan.” The meeting was presided over by the Minister without Portfolio of the Executive Yuan and served to coordinate and consolidate interagency consensus on the National Strategy and Action Plan. These outcomes will guide the country’s ongoing efforts to AML/CFT/CPF.

Our NRA procedures demonstrate adaptability, continuity, repeatability, and the capacity for timely updates in response to evolving circumstances, with the following features: (1) Comprehensive, offering a complete and practical review of key risk factors—including threats, vulnerabilities, and consequences—to assess inherent risk. (2) Inclusive, enabling participation and result-sharing among all public and private sectors involved in AML, CFT, and CPF. (3) User-friendly and easy to understand. (4) Sufficient to address the current national

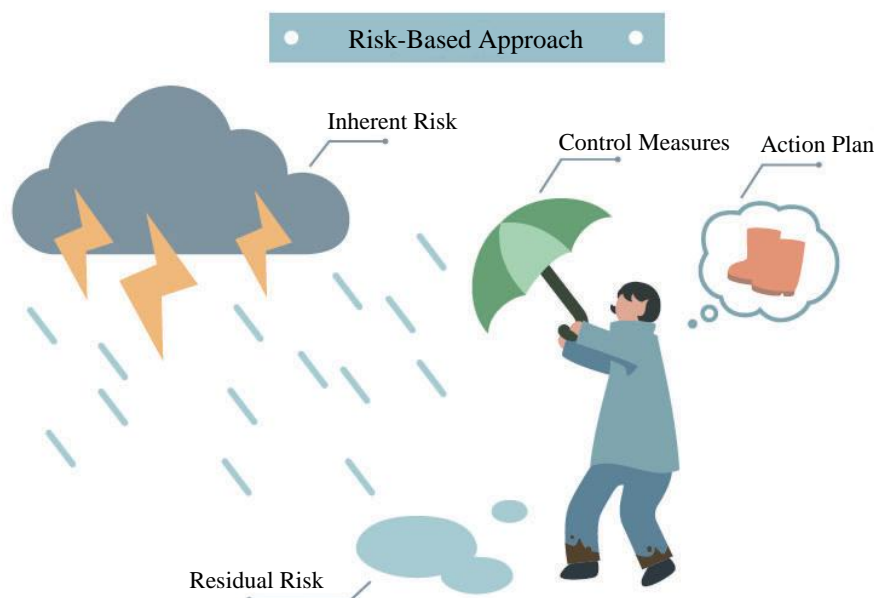
analytical context and any potential data or statistical limitations. (5) Transparent and rigorous. (6) Enabling understanding of residual risk; establishment of risk-based risk-mitigation strategies; formulation of AML, CFT, and CPF policies; and prioritization of interagency coordination actions in alignment with FATF Recommendations.

This report was officially confirmed and finalized in December 2024 and published at the end of 2024 for public awareness, aimed at facilitating the public sector's post-assessment review of internal policies, regulations, and resource allocation; supporting the private sector in implementing AML, CFT, and CPF measures; and ensuring that risk assessments at all levels fully consider the results of the NRA.

The AMLO will continue to advance the national AML, CFT, and CPF risk assessment process on a three-year cycle, formulating and updating the Action Plan based on assessment results to implement risk-mitigation measures. The next NRA report is scheduled for release in 2027.

Section 2. Risk Assessment Methodology

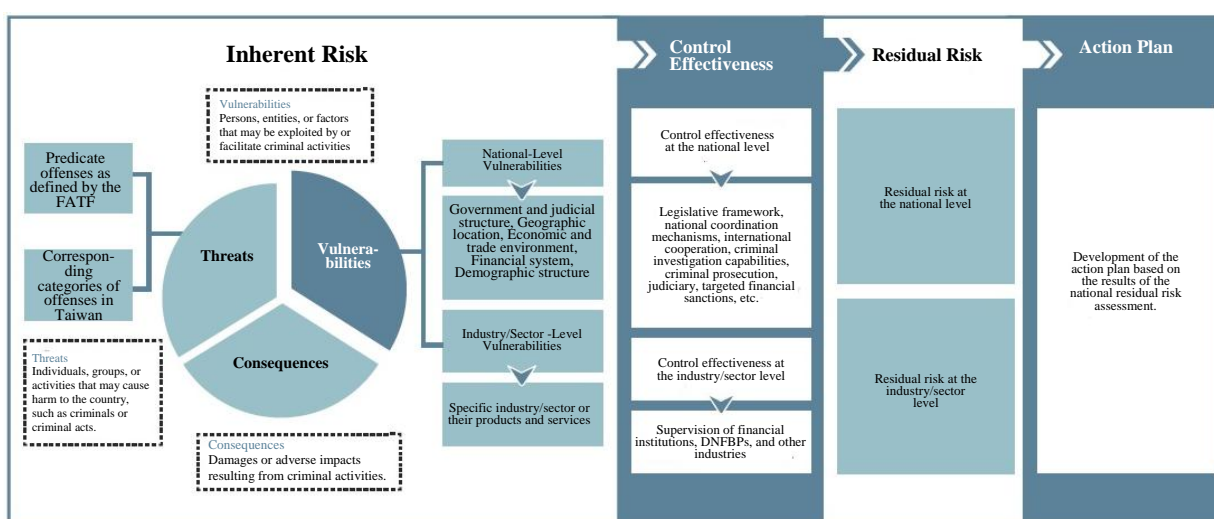
The FATF has established international standards for AML, CFT, and CPF: the FATF 40 Recommendations. Recommendation 1 sets out the fundamental principles of risk assessment. This recommendation urges countries to identify, assess, and understand their ML, FT, and PF risks, with the goal of ensuring effective risk mitigation using risk assessment as the foundation for a risk-based approach (RBA).



There is no single method for conducting an NRA. The key concept is that risk consists of three elements: threats, vulnerabilities, and consequences. Threats refer to individuals, groups, entities, or activities that may cause harm to the country, society, or economy. Vulnerabilities are factors identified from threats that support or facilitate those threats. Consequences refer to the impacts or damages that ML, FT, and PF may cause. In addition, according to FATF NRA

Guidance⁶, countries should prioritize a comprehensive understanding of their threats and vulnerabilities, considering consequences only as part of the overall risk assessment. This approach facilitates the prioritization of mitigation measures and enhances the resilience of the financial and economic environment against ML activities.

In summary, the risk assessment methodology adopted by our country focuses on threats and vulnerabilities for assessing inherent risk while addressing the distinct characteristics of FT and PF risks through separate assessments of “terrorist financing threats” and “proliferation financing threats and vulnerabilities.” Given the special nature of vulnerabilities related to legal persons, legal arrangements/trusts, and NPOs not belonging to specific industries or sectors, these will be addressed in a separate chapter. The assessment of control effectiveness is centered on control capabilities at both the national level and the industry/sector level. The framework for the outputs of the NRA and Action Plan is illustrated below:



1. ML/FT Risk

(1) Inherent Risk

For assessing ML threats, predicate offenses (criminal activities that may generate illicit proceeds) are used as the evaluation items. Each type of predicate offense is assessed using three risk factors: “offender capability,” “scope of money laundering activities,” and “estimated illicit proceeds.” The assessment covers the offender’s demonstrated criminal knowledge, skills, expertise, networks, and resources; the extent to which offenders exploit financial institutions, designated non-financial businesses and professions (DNFBPs), and other sectors for ML; and the scale of illicit proceeds generated through these criminal activities. This risk assessment continues to encompass 24 “money laundering threat” items. The results are rated on a four-point scale; factor and classification definitions are detailed in Annex 3.

⁶ FATF, Money Laundering National Risk Assessment Guidance, <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-National-Risk-Assessment-Guidance-2024.pdf>.coredownload.inline.pdf (Last accessed: November 12, 2024).

For FT threats, Taiwan adopts a threat profile for terrorism (including FT) that includes three risk factors: “terrorist financier capability,” “global scope of activities,” and “estimated annual funds that can be raised in Taiwan”. The analysis also refers to international literature, typology studies, and other (regional or supranational) risk assessments and examines in detail seven indicators: “degree of direct/indirect contact with terrorist organizations,” “knowledge, skills, and expertise in carrying out terrorist financing,” “networks, resources, and capacity for terrorist financing,” “scope and geographic reach of terrorist financing operations,” “estimated annual terrorist financing amount,” “diversity of fundraising and fund-handling methods,” and “extent to which raised funds are used to harm Taiwan’s or international interests.” Factors and classification definitions are detailed in Annex 4.

At the national level, the assessment of ML/FT vulnerabilities uses the following items: “government and judicial structure,” “geographic location,” “economic and trade environment,” “financial system,” and “demographic structure,” providing a comprehensive analysis of Taiwan’s macro-level risk profile and a qualitative analysis of the potential consequences of ML/FT activities.

At the industry/sector level, the assessment of ML/FT vulnerabilities focuses on sectors that may be exploited for ML/FT. Five risk factors are used: “inherent characteristics of the sector,” “products and nature of services provided by the sector,” “nature of business relationships with customers,” “geographic scope of sectoral activities,” and “nature of service delivery channels.” In this assessment, “foreign migrant worker remittance companies” are newly included, “futures trust enterprises” are incorporated into the consolidated assessment of “securities investment trust enterprises” (now “securities investment trust enterprises (including futures trust enterprises)”), and “managed futures enterprises” and “leverage transaction merchants” are merged into the assessment of “futures commission merchants (including managed futures enterprises and leverage transaction merchants)”. In total, there are 36 “ML/FT vulnerability” assessment items. The results are rated on a four-point scale; definitions for each level are detailed in Annex 5.

For legal persons, legal arrangements/trusts, and NPOs, the assessment methodology centers on information transparency. In some cases, a binary risk rating is used, i.e., more/high risk or less/low risk. For legal persons, the assessment covers different types of domestic and foreign legal persons, including the size of the legal person, establishment process, geographic scope of activities, related criminal activities, and disclosure obligations. For legal arrangements/trusts, the assessment covers different types of domestic trusts and foreign legal arrangements, including the nature, structure, establishment method, size, and registration requirements for trust property. The assessment of non-profit organizations covers various types of nationwide NPOs, examining their nature, size, types of donors, organizational structures and links with other sectors, scope of activities, service delivery channels, and types of donation income.

(2) Control Effectiveness and Residual Risk

In evaluating the effectiveness of existing control measures to identify residual risk, the assessment focuses on control capabilities at both the national level and the industry/sector level. At the national level, control capabilities are analyzed based on the following: legal and regulatory frameworks, domestic interagency coordination, international cooperation,

generation and utilization of financial intelligence, law enforcement investigations, criminal prosecution and confiscation of criminal proceeds, judicial effectiveness, targeted financial sanctions, legal persons and arrangements/trusts, and NPOs.

At the industry/sector level, control capabilities are assessed based on the following: licensing and supervision of financial institutions, DNFBPs, and other sectors; risk assessment processes; customer due diligence (CDD); reporting of suspicious transactions and targeted financial sanctions; internal controls; and supervisory measures. The results of the control effectiveness assessment are rated on a four-point scale. However, due to the sensitivity and detail involved in enforcement and supervisory measures, the identified results are available for reference to public sector agencies only.

2. Proliferation Financing Risk

The methodology for assessing PF risk is based on a slightly modified version of Taiwan's existing ML risk assessment approach. The threat profile incorporates three risk factors: "actor capability," "scope of proliferation financing activities," and "estimation of illicit proceeds." Key elements include the actor's demonstrated criminal knowledge, skills, expertise, networks, and resources; the extent to which actors exploit financial institutions, DNFBPs, and other sectors for PF; and the scale of illicit proceeds generated through such activities. For this risk assessment, the Democratic People's Republic of Korea (hereinafter referred to as "North Korea") and Iran remain the primary subjects of evaluation. The assessment results are rated on a four-point scale; detailed definitions are provided in Annex 6.

In the PF vulnerability assessment, consideration was given to Taiwan's specific needs, with reference to selected methodologies developed by RUSI, thereby designing an assessment methodology tailored to the national context. While ML/FT risk assessments typically rely on clear and extensive knowledge and sufficient statistical data, PF risk assessments are often performed with limited information and involve behaviors that are more complex than those associated with ML/FT. Given this context, PF risk assessments require a more flexible classification of vulnerabilities. Taiwan's current PF vulnerability assessment focuses primarily on national-level weaknesses, encompassing five main risk factors: "geographic and environmental factors," "political and social factors," "legal and institutional factors," "economic and technical factors," and "legal persons and arrangements." The design of this methodology also allows for the simultaneous consideration of the mitigating effects of various CPF measures during the vulnerability assessment process, thereby further identifying residual risks. Key assessment content includes the national environmental context, relevant legal frameworks, the status and challenges faced by financial institutions, DNFBPs, and related industries in implementing targeted financial sanctions, as well as the risk awareness of both public and private sectors. The assessment results are rated on a three-point scale; detailed definitions are provided in Annex 7.

Chapter 4. Overview of Risk Assessment Results

At the national level, the results of the NRA for ML, FT, and PF enable the country to review the adequacy of existing regulations, allocation of resources among competent authorities, and current control measures, as well as to determine whether adjustments are needed to effectively address the FATF 40 Recommendations within the limits of available resources.

The outcomes of the national-level risk assessment also support competent authorities in evaluating the rationality of risk factors and parameter settings when conducting industry/sector risk assessments, and they assist the private sector in performing institutional risk assessments. This ensures both horizontal coordination in policy implementation and resource allocation among national competent authorities and vertical alignment from the national to public sector, and even to the private sector, so that ML/FT/PF risk assessments and mitigation efforts are mutually reinforcing.

It is important to emphasize that this risk assessment report discloses only the key points of inherent risk assessment and control measures for ML and FT. In other words, the report aims to provide users with an understanding of Taiwan's risk landscape before the implementation of control measures and the main aspects of risk-mitigation strategies, enabling users to undertake follow-up actions and controls based on the report and allowing competent authorities to adjust the direction of regulations or policy implementation as needed. The actual results of the control effectiveness and residual risk assessments, owing to their sensitive nature and involvement of detailed enforcement and supervisory measures, are available for reference to public sector agencies only. Furthermore, the classification of certain crimes or sectors as high-risk indicates only their level of exposure to ML/FT risks and does not imply that current regulations or control measures are ineffective. For PF risk, both inherent and residual risk assessments are adopted. Subsequent action plans will be developed based on these assessment results to determine the prioritization of various risk-mitigation measures.

Section 1. Money Laundering Risk

The assessment of ML threats revealed that Taiwan faces very high ML risk from ten major types of crime: drug trafficking, fraud, organized crime, tax crimes, securities crimes, illegal gambling, underground banking, smuggling, corruption and bribery, and intellectual property crimes. Third-party ML is also classified as a high-risk crime.

The assessment of ML vulnerabilities revealed that Taiwan's environment—characterized by democracy, freedom, active financial and economic development, and a wide variety of consumer payment instruments—makes certain sectors more susceptible to abuse for ML activities. Industries/sectors with very high vulnerabilities include the following: offshore banking units (OBUs), virtual asset service providers, and domestic banks. Industries/sectors with high vulnerabilities include 12 units: offshore securities units (OSUs), foreign bank branches in Taiwan, offshore insurance units (OIUs), securities firms, jewelry businesses, postal institutions handling savings and remittances, life insurance companies, accountants, lawyers, third-party payment service providers, real estate brokerages, and agricultural financial institutions (including the Agricultural Bank of Taiwan, credit departments of farmers' and fishermen's associations).

In industry/sector activities, due to the particular characteristics of legal persons, legal arrangements/trusts, and non-profit organizations (NPOs), a separate risk assessment was conducted to understand their risk of abuse. Legal persons—Risk of abuse as criminal channels has increased in recent years owing to insufficient information transparency, particularly among non-publicly traded companies and limited companies, which are considered higher risk. Legal arrangements/trusts—Different types and relative risk levels exist depending on classification. Among these, non-business trusts (distinguished by the type of trustee) and private trusts (distinguished by the purpose of establishment), which are considered higher risk, while foreign legal arrangements/trusts require ongoing attention. NPOs—three types are considered higher risk: civil associations, national religious foundations, and social welfare foundations.

Section 2. Terrorist Financing Risk

Regarding the identification of terrorist financing threats, from 2021 to 2023, no FT cases occurred domestically, nor were there any instances of terrorists or terrorist organizations conducting activities in Taiwan. Taiwan's population structure has remained stable. In recent years, the proportion of foreign immigrants has increased; however, population movement is primarily driven by employment needs (according to the Ministry of Labor, as of December 2023, there were 753,430 migrant workers in Taiwan). Furthermore, Taiwan has a harmonious and diverse society in terms of religion, lifestyle, and language, with no evidence indicating any connection to terrorist activities or FT. Overall, the risk of FT is considered “low.”

Section 3. Proliferation Financing Risk

PF activities pose threats to regional security and socioeconomic stability. Taiwan's geographic location and economic conditions may be conducive to such activities; however, as a responsible member of the international community, the country has consistently complied with United Nations Security Council (UNSC) sanctions and implemented FATF Recommendations to combat PF. Domestically, Taiwan is committed to strengthening relevant laws and systems; externally, it actively cooperates with international partners to jointly combat PF activities.

This risk assessment has identified that the primary PF threat to Taiwan is related to activities involving North Korea. In addition to financial institutions and designated non-financial businesses and professions (DNFBPs), several other industries have been identified as potentially involved in or vulnerable to exploitation for PF, including shipping, charter trade, customs brokerage, commodity supply, marine fuel, and virtual asset service providers. Challenges remain in ensuring the transparency of legal persons and arrangements or trusts, particularly in identifying beneficial owners. Both public and private sectors should continue to raise awareness and strengthen measures to mitigate PF risks. Additionally, some regulations and measures related to PF still require further review and revision. Overall, Taiwan's PF risk is rated as “medium” with respect to North Korea and “low” with respect to Iran.

Chapter 5. Risk Assessment Results: Money Laundering and Terrorist Financing Threats

Section 1. Money Laundering Threats

Assessment of ML threats revealed that Taiwan faces very high threats from ten major types of crime: drug trafficking, fraud, organized crime, tax crimes, securities crimes, illegal gambling, underground banking, smuggling, corruption and bribery, and intellectual property crimes. Third-party ML is classified as a high-threat crime. To help users prioritize resources and develop appropriate risk-mitigation measures for higher-risk and emerging areas, this section describes the ten very high threats and one high threat.

Overview of money laundering threat ratings:

| Money Laundering Threat Rating Table | | | |
|--|---|--|--|
| Low | Medium | High | Very High |
| <ol style="list-style-type: none"> Extortion Snatching and Robbery Counterfeiting currency Murder and Aggravated assault Piracy | <ol style="list-style-type: none"> Illicit arms trafficking Environmental crime Theft Forgery Dealing in stolen property Human trafficking Sexual exploitation Kidnapping, illegal restraint, and other offenses against personal liberty | <ol style="list-style-type: none"> Third-party money laundering | <ol style="list-style-type: none"> Drug trafficking Fraud Organized crime Tax crime Securities crime Illegal gambling Underground banking Smuggling Corruption and bribery Intellectual property crime |

1. Very High-Risk Threat: Drug Trafficking

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

Over 70% of the narcotics seized in Taiwan are imported. Seizure data show that heroin, cannabis, methamphetamine, and ketamine pose the most significant harm to the public. Notably, due to the relative ease of obtaining cannabis, the annual number of cannabis seizures has reached a record high. In recent years, there has also been a growing trend of domestic cannabis cultivation, driven by increasing cases of individuals purchasing cannabis seeds through foreign websites or the dark web. Additionally, another emerging trend among drug trafficking organizations is the importation of non-regulated precursor chemicals to replace previous methods involving the smuggling of Class IV precursor chemicals for domestic drug production, in an attempt to evade customs inspections and law enforcement investigations.

The main participants in drug trafficking activities include individuals and organized crime groups, with criminal organizations formed through strategic alliances among Taiwanese and overseas Chinese groups holding more significant influence. Domestic drug smuggling syndicates are becoming more international and complex, comprising members from Taiwan, Mainland China, Japan, and Southeast Asia, including drug kingpins and gangs. Their diverse organizational structures and specialized divisions of labor make it difficult to fully uncover these drug trafficking networks.

Since 2022, as countries have eased border controls following the COVID-19 pandemic, both maritime smuggling and cases in which travelers conceal drugs within their bodies or luggage have risen substantially, indicating that drug smuggling activities and volumes have returned to pre-pandemic levels. The primary source of drug smuggling was Mainland China in 2021 and 2022 and Thailand in 2023. Statistics reveal that heroin mainly obtained from Thailand; amphetamine from domestic production and imports from Malaysia, Vietnam, and Myanmar; cannabis from Canada and Thailand; ketamine from Thailand and Myanmar; and precursor chemicals from Mainland China.

To evade anti-narcotics investigations, apart from a minority of “drugs-for-drugs” transactions, domestic drug offenders typically conduct transactions via cash handover, front accounts, or underground casinos. For cross-border smuggling, illicit proceeds are transferred via foreign front accounts, underground banking services, and virtual assets, with e-commerce platforms, social media, and messaging apps commonly being used as transaction channels. Once transactions are complete, laundering is conducted through jewelry dealers, underground banking operators, wire transfers through front accounts, shell companies, offshore casinos, and the physical transportation of cash in and out of the country. In the case of cross-strait drug transactions, the main laundering conduits include cross-strait underground banking operators; jewelry dealers; Taiwan branches of Hong Kong trading companies; companies conducting cross-strait business; and casinos in Hong Kong, Macau, or the Philippines.

The leading countries or regions for outgoing and incoming criminal proceeds vary by drug type; however, overall, Mainland China, Hong Kong, Macau, and Southeast Asian countries (including Thailand, Malaysia, Vietnam, Cambodia, the Philippines, Laos, and Myanmar) are the primary jurisdictions involved. In recent years, Canada, the Netherlands, and the United States have also emerged as key outflow locations for proceeds from drug purchases.

The estimated criminal proceeds were approximately NTD11.7 billion in 2021, NTD18.4 billion in 2022, and NTD22.4 billion in 2023.

Case Study

Since March 2023, Group A, to which Person A belongs, has been mailing packages containing Class II controlled cannabis from Vietnam to Taiwan for resale and profit. Members of Group A were instructed to deposit over NTD700,000 in drug sale proceeds into front accounts via non-passbook cash deposits and then transfer the funds through multiple layers to unidentified recipients in order to obscure the money trail.

Source: Investigation Bureau, Ministry of Justice

2. Very High-Risk Threat: Fraud

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

Fraud is one of the most common types of crime globally, and proceeds from fraud are also among the primary targets for ML. In Taiwan, fraud takes many forms, including loan fraud, investment fraud, international trade fraud, real estate transactions, health insurance fraud, insurance fraud, bankruptcy fraud, check fraud, online fraud, telecom fraud, and illegal fundraising. Among these, investment fraud is particularly widespread, with perpetrators enticing victims by promising returns such as bonuses, interest, dividends, returns, or other rewards disproportionate to the principal, inducing them to join as shareholders or under various titles and solicit funds from a broad or unspecified audience. Criminals have increasingly engaged in fraud through the Internet, virtual assets, e-commerce, and telecommunications, which has evolved with technological developments into corporatized criminal groups.

Perpetrators may operate alone or as part of a criminal group. Typical schemes involve online shopping scams, third-party fraud, and impersonation of friends or family, often leveraging online platforms and messaging apps to deceive victims and collect proceeds through front accounts. Fraud rings typically possess internal management structures with strict organizational division of labor; they employ tactics such as fake investments, romance-investment fraud, impersonation of authorities, and installment payment deactivation to defraud victims.

In recent years, fraud has become progressively corporatized, layered, cross-border, and specialized, with increasing convergence with other predicate offenses. Sophisticated crime rings exploit rapid advances in information technology and financial liberalization, continually updating their methods to persuade victims to transfer funds into designated front accounts under various pretexts. Money mules are then directed to withdraw cash in Taiwan, while upstream and downstream members operate independently. This professional division of labor makes it difficult for law enforcement to identify key ringleaders. Fraud organizations also recruit personnels with expertise in finance, law, and information technology to evade detection, making them highly vigilant. These actors possess a high level of knowledge concerning the laundering of criminal proceeds. Illegal fundraising crimes similarly exploit the Internet and emerging technologies, enticing victims via investment schemes; such perpetrators likewise possess significant ML knowledge.

Fraud rings routinely employ diverse channels to conceal and dissipate criminal proceeds; they act in a systematic and compartmentalized manner and cover diverse sectors such as services, telecommunications, information technology, and financial sector, resulting in high complexity. Their activities transcend borders; they use cash withdrawals or staged wire transfers to create multiple layers in the money trail and evade detection or conduct sham transactions with overseas parties. ML is effected through banks and underground banking providers or by using offshore banking unit (OBU) accounts to transfer criminal proceeds abroad. Domestically, principal offenders behind fraud operations may create legitimate companies to disguise illegal income; purchase high-value metals, jewels, or real estate; reinvest illicit gains; or directly expend the proceeds on luxury vehicles, properties, and other assets. In recent years, there have been cases of laundering fraud proceeds abroad by converting them into Bitcoin and instances of online lending platforms being implicated in fundraising crimes.

A portion of the fraud proceeds is laundered overseas through underground banking or casinos. Key outflow regions and countries include Mainland China, Hong Kong, Macau, Thailand, Malaysia, Indonesia, Japan, South Korea, and the United States. In recent cases, funds have also been laundered to Cambodia through virtual assets. The primary sources of illicit funds also include Mainland China, Hong Kong, and Macau. Owing to linguistic and demographic factors, most overseas victims are from Mainland China; consequently, related criminal proceeds predominantly flow from Mainland China back to Taiwan via various ML channels. For illegal fundraising crimes, the inflow and outflow of illicit gains are principally domestic, with minimal changes over the past three years.

According to statistics from the Criminal Investigation Bureau of National Police Agency on telecom fraud, estimated criminal proceeds amounted to approximately NTD5.6 billion in 2021, NTD7.3 billion in 2022, and NTD8.8 billion in 2023. Including illegal fundraising crimes, the annual average reaches approximately NTD70 billion.

Case 1

In March 2023, Person A joined the A fraud syndicate. The syndicate initially lured victims by falsely claiming on the Internet that investments in virtual assets would generate high returns. Deceived by this scheme, the victims followed instructions to create wallet addresses on an online platform operated by the A fraud syndicate. Members then directed victims, using scripted communication techniques, to purchase virtual assets from designated fake traders recruited by Person A, often at prices exceeding market value.

Following instructions from the fraud syndicate, Person A instructed the fake traders to advertise on social media and exchange platforms. The fake traders met victims in person to conduct virtual asset transactions. Upon transferring (“flying”) the virtual assets to wallet addresses established on the syndicate’s online platform, the assets were immediately moved to anonymous wallets controlled by the syndicate and then successively transferred upstream within the group. The syndicate’s upstream members subsequently returned the virtual assets to Person A, who sold them to the next group of victims, earning a cash spread. After deducting this spread, Person A, via a designated “collector,” transferred the proceeds upstream to purchase virtual assets from an exchange, which were then wired to the syndicate’s overseas wallets. The syndicate cashed out through undisclosed exchanges, thereby creating breaks in the fund flow and obscuring or disguising the illicit destinations of the fraud proceeds.

Source: Taiwan High Prosecutors Office

Case 2

Company A operated a lending matching platform, raising capital from the public through online lending and investment subscriptions. It fabricated false high-yield debt claims for an unspecified pool of investors, thereby deceiving investors into paying for nonexistent claims. Company A subsequently paid monthly interest to investors based on these purported investments. However, beginning in late 2022, Company A ceased paying interest and principal as scheduled, resulting in investors losing their entire investments. The total funds raised exceeded NTD150 million.

Source: Criminal Investigation Bureau, National Police Agency

3. Very High-Risk Threat: Organized Crime

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

The primary organized crime groups in Taiwan are the Heavenly Way Alliance, the Bamboo Union, and the Four Seas Gang. Illicit activities conducted by these organizations are increasingly diversified, including acting as muscle for others, extortion of businesses, operation of sex industries, underground casinos, underground money lenders, investment firms, security companies, debt collection agencies, lottery operations, video game stores, Internet cafés, sand and gravel yards, landfill sites, cable television operations, violent manipulation of public construction contracts, coercive takeovers of listed companies, aggressive interference in urban redevelopment, smuggling of drugs and firearms, acting as election brokers or candidates, violent election disruption, operation of underground casinos combined with violent debt collection, intimidation and extortion, extortionate compensation claims, intrusion into school campuses, illegal extraction of national resources, and other activities posing serious threats to public safety and welfare, alongside various other grave and malicious offenses. Criminal activities conducted by organized crime groups are not limited to coercive or violent acts; profit-driven motives are also a distinguishing characteristic of organized crime.

According to the types of criminal involvement, organized crime groups in Taiwan often use online gambling, underground money lending, casinos, and related companies to facilitate the movement of funds. Groups asserting territorial dominance are known to extort cash for protection fees, further complicating the traceability of these financial flows. In cases involving drug trafficking or telecom fraud, domestic transactions are primarily conducted in cash to evade detection by law enforcement agencies; for cross-border criminal organizations, the separation of people, goods, and money ensures transactional security, with ML channels including wire transfers through front accounts, shell companies, jewelry dealers, underground banking operators, offshore casinos, and physical transport of cash across borders.

Regarding estimates of criminal proceeds, given that organized crime encompasses multiple offense types, the proceeds from drug trafficking, fraud, and violent crime cases are aggregated for estimation, amounting to approximately NTD2.2 billion in 2021, NTD2.0 billion in 2022, and NTD5.4 billion in 2023.

Case Study

Since August 2021, A, the leader of an organized crime group, has directed subordinates to employ violent, coercive, and intimidating tactics to collect commissions and fabricate pretexts to secure illegal profits. From March 2022, he collaborated with overseas fraud syndicates and led members to Cambodia to join forces with local fraud groups; he left group members there to scam victims in Europe and the United States through romance fraud or fake investment schemes using social media or messaging apps. The ring also lured young Taiwanese to Cambodia under the guise of high-paying hotel jobs, recruiting them to work in fraudulent virtual asset investment call centers. They employed violence and intimidation to manage, assault, or threaten victims who underperformed or resisted cooperation.

Source: Criminal Investigation Bureau, National Police Agency

4. Very High-Risk Threat: Tax Crimes

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

Tax crime cases are typically characterized by the evasion of tax payments through fraud or other improper means or by assisting others in evading taxes. Common methods include the following:

- (1) Tax crimes involving individuals, companies, and legal entities: Falsifying costs, expenses, or input tax amounts without corresponding sales or payment transactions; forging or altering uniform invoices; conducting transactions under others' names; concealing assets; or dispersing income.
- (2) Assisting others in tax evasion: Creating shell businesses using numerous straw persons to issue false invoices to companies or legal entities; dispersing income to evade individual income tax, corporate income tax, and business tax; or hiding the true nature of commercial transactions by fraudulently claiming tax refunds.
- (3) Fraudulent export tax rebates: Exploiting government policies that encourage export tax rebates by declaring artificially high export amounts on low-value goods or waste products to defraud tax refunds.

Tax offenders possess comprehensive knowledge of domestic commercial transaction patterns and extend their targets internationally through sham commercial schemes—such as international trade or triangular transactions—to obscure the flow of goods and funds and evade detection by judicial authorities. To conceal assets and divert income, tax offenders in Taiwan are often well-versed in domestic tax assessment and financial transactions, constituting white-collar crimes. Participants usually use money laundering techniques to transfer illicit gains to themselves or companies under their control.

Tax offenders frequently open a large number of front accounts domestically and fabricate transactions to create financial flows. When concealing personal illicit income, they commonly withdraw large sums in cash or use methods that create gaps in transaction trails, thereby obscuring funds and evading detection. Moreover, they establish shell companies in Mainland China, Hong Kong, Macau, and other regions and countries such as the Philippines to commit tax fraud—claiming false exports to fraudulently obtain export tax rebates or using offshore bank accounts to evade scrutiny before remitting funds back to Taiwan through underground banking or sham transactions. Currently, the rate of third-party assistance in tax evasion is low, with limited participation from DNFBPs in tax crime cases. To date, there is no evidence of tax crimes facilitated through domestic or offshore trusts, nor through the use of emerging technologies. According to law enforcement analysis, Mainland China, Hong Kong, Macau, and the Philippines are all countries or regions associated with the inflow and outflow of criminal proceeds.

According to data from the Investigation Bureau of Ministry of Justice, the estimated average annual criminal proceeds from 2021 to 2023 amounted to approximately NTD7.6 billion, while proceeds from inciting or aiding tax evasion averaged around NTD460 million per year.

Case Study

A, B, C, and D were actual partner-investors in Medical Group A. To exploit lower progressive income tax brackets and reduce their consolidated tax liabilities, they artificially increased the number of partners to disperse joint business income. As part of this scheme, they recruited E, F, and G to pose as partners, using the partnership façade to further divide the joint business income originally belonging to A, B, C, and D. E, F, and G were fully aware that they did not contribute capital as partners and were merely salaried physicians employed by Clinic B; however, they still agreed to be listed as nominal partners of Clinic B. In addition to splitting the joint business income among A, B, C, and D, E, F, and G also reported business income as part of their comprehensive income, enabling them to claim higher expense deductions and qualify for lower progressive tax brackets, thereby potentially evading taxes. All seven individuals were aware that in addition to the regular salaries transferred monthly from Clinic B's account at Bank C, partner and employed physician compensation also included other business income that should have been accurately declared and reported in the Statement of Business (Other) Gains and Losses. H and I, who either received performance bonuses or invested in Medical Group A, also received income outside of regular salary. To evade individual consolidated income tax for 2021 and 2022, these nine individuals, with the assistance of H and I in bookkeeping, filed false statements, sham partnership agreements, and consolidated income tax returns with the tax authorities under the Ministry of Finance, thus evading significant tax payments.

Source: Taiwan High Prosecutors Office

5. Very High-Risk Threat: Securities Crimes

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

The types of offenses that violate the Securities and Exchange Act include insider trading, market manipulation, securities fraud, dissemination of false or misleading information, and corporate asset stripping. The legislative purpose of these provisions is to safeguard investors' equal access to information and uphold a fair and orderly securities market. Accordingly, specific provisions are established for corporate insiders—such as directors, supervisors, managers, and other key personnel or recipients of material non-public information (tippees)—who possess information not equally accessible to the general investing public. These provisions aim to prevent insiders from exploiting such information asymmetry for unlawful gain and thereby from inflicting harm on public market investors.

The primary perpetrators of insider trading are individuals within a company who possess knowledge of significant positive or negative information, as well as external professionals—such as lawyers, accountants, and financial advisors—who assist in corporate mergers and acquisitions, as well as those who obtain such information from the aforementioned individuals. Insider trading commonly involves individuals with access to material information executing stock trades of the target company through accounts held by friends, family members, or employees during the restricted trading period (i.e., prior to public disclosure or within 18 hours after disclosure). They then conduct reverse transactions following disclosure to capitalize on illegal price differentials.

The principal actors in market manipulation are stock traders with substantial capital, although they often leverage funding from Class C loan providers (known as “funding sources”) to enhance their operational leverage. These manipulators create artificial supply and demand imbalances by continuously placing high buy and low sell orders, engaging in matched trading, or even disseminating false information, resulting in abnormal surges or drops in the target company's stock price. The traders then profit by capitalizing on the resulting significant price differentials.

Cases of securities fraud and financial statement misrepresentation are primarily committed by company heads, general managers, and chief financial officers. These individuals engage in fraudulent capital increases and capital verification processes, followed by the issuance and trading of the company's shares. Some companies, in attempts to inflate financial performance, engage in fictitious transactions to overstate revenue, distorting financial statements and misleading investors' decisions, ultimately converting “window-dressed” stocks into illicit monetary gains.

The main perpetrators of asset-stripping cases are senior decision-makers such as company heads, general managers, and chief financial officers. A common method involves conducting transactions with related parties (companies) under fabricated or markedly unfavorable terms compared with normal market conditions, thereby misappropriating company assets.

Although the above criminal methods are conducted via financial accounts, once assets are transferred out, suspects often create a break in the transaction trail by withdrawing cash. The illicit proceeds are then used to purchase high-value goods such as precious metals or real

estate, laundered through underground banking channels or routed via sham transactions with offshore third parties. Funds are also transferred out of the country through personal or third-party OBU accounts or sent abroad via casinos. Only a small portion of the illicit gains is retained domestically and used to purchase real estate or precious metals.

Estimated criminal proceeds from securities crimes were approximately NTD5.1 billion in 2021, NTD4.8 billion in 2022, and NTD2.8 billion in 2023.

Case Study

Mr. A served as the chairman and general manager of publicly listed Company A. Mr. B was the director of Company A and the supervisor of Company B. Since 2017, Mr. B functioned as the de facto operator of Company A and was also the actual controlling party behind several offshore entities, including Company C. Acting on Mr. B's instructions, Mr. C, a manager at Company B, oversaw triangular trade transactions between Company A and the aforementioned offshore entities.

Starting in 2012, Company A experienced a steady decline in revenue. Between 2018 and 2020, in an effort to maintain the appearance of robust earnings, Mr. B, together with Mr. A and Mr. C, arranged fictitious triangular transactions between Company A and the C companies under Mr. B's control. These transactions falsely inflated Company A's revenue by over NTD1.3 billion, accounting for 96.67% of the total revenue reported in Company A's financial statements for 2018 through 2020. Mr. B then used the falsified performance as promotional material and instructed Mr. C, who was aware of the scheme, to place buy orders through the nominee securities accounts that he controlled. This market manipulation led to a surge in Company A's stock price—from NTD21.90 per share on a given day in 2020 to NTD43.40 per share on a given day in 2021, representing a 98.17% increase and a 106.84% price fluctuation—both exceeding those of comparable stocks and market indices during the same period. The illicit profits generated from this market manipulation amounted to more than NTD116.93 million.

Source: Investigation Bureau, Ministry of Justice

6. Very High-Risk Threat: Illegal Gambling

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

Gambling is a reciprocal crime in which offenders engage in gambling activities involving assets in public venues or places accessible to the public. In some cases, individuals also provide gambling venues with the intent to profit. In the case of organized crime, illegal gambling operations may involve online gambling companies and their associated betting platforms or collections centers ("water rooms"), as well as intermediaries or agents. In recent years, due to the widespread popularity of online gambling, most offenders have acted as part of organized criminal groups that integrate both information and financial flows to facilitate illegal operations. Traditional, individual gambling activities tend to involve minimal ML risks as offenders typically lack the relevant knowledge. In contrast, casinos and online gambling platforms operated by criminal organizations often exhibit far greater awareness of, and capacity for, ML.

Online gambling crime syndicates commonly use offshore front accounts to allow gamblers to place bets; alternatively, they facilitate deposits via designated third-party payment service providers. Such operations are frequently supported by cross-border data centers and make use of virtual private network (VPN) technology to circumvent detection. Gambling funds and illicit proceeds are transferred or laundered through banks, third-party payment service providers, virtual asset service providers, or underground banking channels.

Estimated criminal proceeds from illegal gambling activities were approximately NTD11.8 billion in 2021, NTD1.9 billion in 2022, and NTD1.2 billion in 2023.

Case 1

Starting in 2020, a South Korean national (Person A) established a base of operations in Taichung City, Taiwan, and recruited ten Taiwanese citizens to assist with facilitating deposits and crediting betting points for users on an online gambling website. They also helped link the offshore gambling site with third-party payment services. Once the offshore gamblers remitted criminal proceeds into Korean-based front accounts, Person A's team used software systems in Taiwan to convert the funds into betting credits at a 1:1 rate. When gamblers won, the site's backend platform used online banking tools linked to the same Korean front accounts to remit illegal winnings directly to the gamblers' designated bank accounts in Korea. Through this method—utilizing Korean front accounts, point conversion programs, and backend network platforms—Person A handled over NTD280 million in criminal proceeds. The criminal funds were then transferred to a computer system at the local base in Taiwan and disguised as legitimate income, making financial tracing difficult and concealing the illicit origin of the funds.

Source: Investigation Bureau, Ministry of Justice

Case 2

In 2022, authorities found that shortly after opening an account, Company A began receiving frequent, high-value transfers from numerous unidentified individuals, totaling more than NTD190 million within 2 months. Many of these transfers carried notes such as “gaming,” “prepaid,” and “online casino,” and the funds were primarily routed to two unrelated entities—Company B and Company C. One of the accounts under Company C was suspected to serve as a gambling deposit account. An investigation revealed that a 13-member illegal gambling syndicate, known as a “water room,” had established five shell companies, including Company A. The group operated under the guise of third-party payment collection services, handling inward and outward funds for illegal gambling platforms. Through these shell entities, they laundered and concealed criminal proceeds amounting to NTD650 million.

Source: Criminal Investigation Bureau, National Police Agency

7. Very High-Risk Threat: Underground Banking (Informal Value Transfer Systems)

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

Underground banking refers to the unauthorized operation of foreign exchange services by criminals who conduct cross-border currency conversion or payment settlement without physically transferring cash. These activities typically involve offering exchange rates and service fees lower than those of formal banking channels and rely on settlement between affiliates or designated individuals in different jurisdictions to conduct the transfer or conversion of different currencies or to facilitate the disbursement and receipt of funds across borders.

Underground banking offenders may establish ostensibly legitimate companies domestically or overseas, either independently or as part of other business ventures. By fabricating payments for trade or wages, they employ mirrored bookkeeping across two jurisdictions to offset transactions and conceal the true movement of funds, thereby exhibiting a notable level of ML sophistication. They may also operate multiple front accounts in Taiwan to process remittance transactions. To settle payments with offshore branches or designated individuals, funds are sometimes exchanged into New Taiwan Dollars or foreign currency and physically transported abroad by cash couriers; alternatively, they are settled using others' remittance and OBU accounts. Such criminal activities frequently involve blending illicit proceeds with legitimate business transactions, particularly involving Taiwanese or Chinese companies, making it difficult to distinguish between lawful and unlawful funds.

Domestically, these schemes are often found in stores that sell imported goods to foreign nationals. Cross-border underground banking networks have also been uncovered across Mainland China and Southeast Asia and within trade, investment, or jewelry businesses, logistics companies, or illegal gambling syndicates. The primary source and destination jurisdictions for these illicit flows include Mainland China, Hong Kong, Macau, Vietnam, Indonesia, Cambodia, the Philippines, Thailand, and Myanmar, with Mainland China representing the largest share. Compared with the previous risk assessment period, recent underground banking operators have increasingly used logistics companies as a front to facilitate cross-strait financial transactions, further complicating law enforcement efforts. As criminal methods evolve with advancements in technology, offenders are increasingly exploiting virtual assets (valued for their anonymity and ease of cross-border transfer) and cold wallets (favored for their portability and concealability) to transfer illicit proceeds, which hampers effective detection and interdiction.

Underground banking schemes can involve flows in the range of tens to hundreds of billions of New Taiwan Dollars. However, offenders typically take a percentage of these flows as commission, thereby making the actual estimated criminal proceeds range from tens of millions to several billion New Taiwan Dollars.

Case 1

Since 2021, Person A, a Taiwanese operator of a cosmetic clinic business in Mainland China, has engaged in underground banking activities using his business as a front. After receiving NT dollars from Person B in Taiwan, A settles the equivalent RMB amount owed by B to a seller in China. This repeated pattern of converting funds across jurisdictions, often involving different currencies, enables Person A to settle Person B's debt obligations and laundering funds overseas. The total volume of underground remittances involved in this scheme is estimated in the tens of millions of New Taiwan Dollars.

Source: National Police Agency, Ministry of the Interior

Case 2

Person A, the registered and actual operator of Company A, also controls six subsidiary companies, including Company B. While Person B is A's nephew, ultimate control remains with Person A.

A's group established a network of logistics companies as a front and set up operational bases in Mainland China. Partnering with a cooperating entity, Company C, Chinese employees relayed current exchange rates between RMB and NTD to A via WeChat. A then provided these rates to Taiwanese buyers based on the Taiwan Central Bank's reference rates. Upon receipt of goods, Taiwanese storeowners, such as Person C, paid for products sourced from Chinese sellers via Company A's local office in RMB. The equivalent NTD amounts were subsequently deposited into 30 bank accounts held under A's name and those of the six subsidiary companies.

Mainland clients seeking to remit payments to Taiwanese vendors delivered RMB cash to Company A's China office. A and B then transferred the equivalent funds to the personal accounts of eight designated Taiwanese recipients, including Person D. The cumulative amount of inward and outward transactions totaled over NTD19.9 billion.

To evade detection, A utilized the accounts of the six subsidiary companies, along with personal accounts held under A's and B's names, to receive and transfer funds. This layering of transactions obscured the true origins and destinations of the illicit funds, thereby facilitating the laundering of proceeds from underground banking operations.

Source: Investigation Bureau, Ministry of Justice

8. Very High-Risk Threat: Smuggling

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

Smuggled goods generally fall into two major categories: agricultural/aquatic/livestock products and other contraband. Among agricultural products, aquatic products account for the largest volume, followed by agricultural goods and livestock. The most common smuggling

method for aquatic products involves Taiwanese fishing vessels traveling to Mainland China or purchasing fish catches from Chinese fishing vessels at sea. The smuggled items are typically high in economic value, with lobsters being the most frequently smuggled product. Agricultural product smuggling often involves concealed shipments in containers or false customs declarations. The types and volumes of goods smuggled are largely driven by market demand, with shredded shiitake mushrooms and shredded black fungus being the most frequently intercepted items in recent years. Other contraband includes cigarettes and alcoholic beverages. Unlicensed white-brand cigarettes constitute the majority, while smuggled alcohol accounts for a smaller proportion.

Individual smuggling is commonly conducted on a small scale by petty couriers, while smuggling rings often set up shell companies to reduce the risk of detection and evade duties such as customs tariffs, business tax, tobacco and alcohol tax, profit-seeking enterprise income tax, and tobacco health and welfare surcharges. Smuggling rings usually collect payments from buyers through front accounts at financial institutions or informal underground financial systems. Downstream members—whether individuals or members of smuggling networks—typically spend illicit proceeds directly and exhibit little to no understanding of ML techniques, and no cases involving the concealment or layering of criminal proceeds have been identified. However, mid- to high-level members of smuggling groups generally demonstrate greater ability to obscure financial flows.

Estimated criminal proceeds were approximately NTD800 million in 2021, NTD700 million in 2022, and NTD600 million in 2023.

Case

In 2023, Taichung Customs under the Customs Administration intercepted a batch of prefabricated container housing units imported from Mainland China. Using container scanning equipment, officers discovered hidden compartments within the units concealing 3,360 kilograms of shredded shiitake mushrooms from China, with an estimated market value of NTD3.02 million.

Source: Customs Administration, Ministry of Finance

9. Very High-Risk Threat: Corruption and Bribery

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

Corruption and bribery offenses involve public officials who—in the course of performing statutory duties such as handling procurement, supervising and managing public works projects, or conducting investigation and enforcement actions—directly or indirectly solicit or accept bribes or other undue benefits. While corruption offenses are often committed by individual public servants, in certain departments—such as local police departments, public infrastructure agencies, and building administration offices—lower-level officials with limited authority may engage in collective bribery to accommodate the demands of those offering bribes. Primary offense patterns and methods include the following.

- (1) Construction and engineering personnel: Engage in corrupt conduct by inflating procurement prices or quantities, leaking confidential bidding information such as reserve prices or the identities of evaluation committee members, accepting hospitality from contractors, collecting kickbacks, facilitating contract awards for selected vendors, assisting in the falsification of construction inspection reports or acceptance records, and enabling fraudulent acceptance processes so that contractors may request payment and obtain unlawful gains.
- (2) Environmental protection personnel: Engage in corrupt activities by accepting bribes in the course of performing their duties such as waste recovery and disposal, environmental inspections, or environmental impact assessments, or by abusing their authority under false pretenses to extort money or other benefits.
- (3) Funeral Services Personnel: Certain individuals responsible for funeral affairs exploit their authority over private funeral facility management, collection of public facility usage fees, and approval of cemetery use and burial permits to engage in corrupt practices. These include holding undisclosed ownership interests (concealed shareholding), misappropriating assets entrusted to them by virtue of their position, or accepting bribes to help illegal operators or cemetery applicants obtain the required permits.
- (4) Elected Representatives: Corrupt conduct among elected officials includes the misuse of public subsidies by claiming assistant salaries under fictitious names despite no actual assistant work being performed and diverting the public funds for personal use. It also encompasses abusing one's official capacity or political influence to lobby, pressure, or intervene in the work of public officials in exchange for bribes from business operators or directly soliciting bribes from operators under false pretexts.
- (5) Construction Regulation Officials: These officials exploit their authority over the review and issuance of building and occupancy permits, accepting bribes to ensure certain developers obtain the required licenses and permits through improper means.
- (6) Civil Registry and Land Administration Officials: Corrupt land officials may collude with developers to illegally reclassify agricultural or forestry land in general agricultural zones into land for other uses, forge cadastral survey maps, overstate base area measurements, or solicit improper fees while performing duties such as land boundary verification and building completion surveys.
- (7) Law Enforcement Officers: Some officers accept bribes to protect illegal operations such as prostitution or gambling. They may also be unlawfully induced to leak personal information about citizens (e.g., vehicle registration data) for improper purposes.
- (8) Judicial Personnel: Judicial officers may abuse their authority over criminal prosecutions and judicial decision-making by accepting bribes or other improper benefits, thereby eroding the integrity of the justice system and diminishing public trust.
- (9) Customs Officers: By abusing their roles in customs clearance, inspections, cargo verification, or taxation, certain customs agents collude with brokers or enterprises to enable illicit express processing or the smuggling of contraband, accepting bribes in return.

- (10) Electoral Bribery: Electoral bribery is a general term for offenses involving the use of money to influence elections. Common forms include bribing candidates, candidates accepting bribes, bribing voters, bribing organizations, or coordinating mass vote-buying operations. Typical methods include cash-for-vote schemes, gift-giving, sponsored trips, or hosted banquets. Candidates or their supporting factions or organizations often distribute cash or gifts to voters through political factions or agricultural and fishing associations. At the grassroots level, local operatives (commonly referred to as vote brokers) monitor election day to ensure that bribed voters fulfill their commitments at the polls. In some cases, travel arrangements or banquet invitations offered during the campaign are excessively lavish and are intended to secure votes.

As Taiwan requires national examinations for entry into civil service positions and many senior officials possess advanced academic or professional backgrounds, public servants who commit corruption-related offenses tend to have higher knowledge of ML techniques. They are well-versed in the regulations and skilled at identifying legal and procedural loopholes. Additionally, corrupt actors often demand bribes in cash, which are then concealed in bank safe deposit boxes or deposited into accounts held by close relatives or trusted associates. Other methods include the use of nominee accounts, offshore funds, conversion into precious metals (e.g., gold), land purchases, or reinvestment into underground money lenders, all of which are carried out to launder proceeds and evade detection.

ML associated with corruption is primarily carried out through banking transactions. In some cases, offenders attempt to conceal illicit proceeds by converting them into gold, real estate, equities, or savings-related insurance policies. Accordingly, financial institutions, jewelry businesses, real estate agents, underground banking operators, offshore funds, and virtual assets may all be involved in laundering proceeds derived from corruption-related offenses.

Estimated criminal proceeds amounted to approximately NTD108.49 million in 2021, NTD126.09 million in 2022, and NTD189.63 million in 2023.

Case 1

Person A, serving as the director-general of a government agency, possessed authority over the planning, zoning, and development of multiple industrial parks. In 2022, despite being fully aware that subcontractors for public infrastructure projects within these parks were to be selected independently by the primary contractors—and that he had no authority to intervene in such decisions—A repeatedly misrepresented the scope of his influence over the developers to Company A, which was actively pursuing subcontracting opportunities. Misled by A's false claims regarding his official capacity, Company A proceeded to give multiple bribes.

Upon learning that his corruption had been reported and fearing a judicial investigation, A sought to conceal part of his illicit proceeds—specifically NTD2 million in cash—by falsely claiming that the funds were intended for stock investments. He entrusted Person B, who was unaware of the criminal origin of the funds, to hold the money. A transferred the entire cash amount to B in installments, after which B deposited the funds into their own bank accounts. This approach was intended to conceal and obscure both the origin and the ultimate destination of the illicit assets. Later, as

media coverage surrounding A's involvement in corruption grew, B grew suspicious about the source of the funds and became concerned about potential personal liability. B withdrew NTD2 million in cash from the accounts and returned it to A. Law enforcement later searched and seized the remaining NTD280,000 in cash, while the whereabouts of the remaining NTD1.72 million remain unknown.

Source: Investigation Bureau, Ministry of Justice

Case 2

In 2021, security personnel (Person A and others) at a detention center under the National Immigration Agency solicited and accepted bribes from detainees, in non-compliance with regulations requiring foreign detainees to deposit valuables above a specified amount with the facility, while retaining only limited cash for personal use. A and others accepted bribes from foreign detainees, allowing those lacking sufficient official funds to receive and keep cash from friends or relatives during visits. To conceal the illicit proceeds, A and others deposited the bribe money into the detainees' bank accounts, maintained possession of the passbooks and chops (account stamps), and instructed their spouses and children to repeatedly make cash deposits and withdrawals. This was done to create breaks in the transaction flow and hide the origin and destination of the illegal funds.

Source: Agency Against Corruption, Ministry of Justice

10. Very High-Risk Threat: Intellectual Property Crime

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

Intellectual property crime in Taiwan primarily encompasses three main types: copyright infringement, trademark infringement, and trade secret misappropriation. Intellectual property crimes involve the following.

- (1) Copyright and trademark infringement offenses mainly involve individuals or companies engaging in unauthorized use of others' photographs, product images, or similar materials on websites or auction pages; downloading and reproducing movies or audiovisual files via peer-to-peer (P2P) software; making these files accessible for public browsing or download on personal websites or blogs; using unauthorized karaoke machines; reproducing textbooks or course handouts; plagiarizing thesis content; selling pirated tutorial CDs and other counterfeit disks; downloading others' software; operating private game servers; imitating others' product designs or artworks; and selling computers preloaded with unauthorized operating system software. Most of these cases are committed by individuals or small-scale businesses. In recent years, with the rapid development of the Internet, these offenses have increasingly utilized applications (apps), digital audiovisual content, and infringing websites as operating models, with perpetrators seeking illegal profits through digital media. As for trademark infringement, such

offenses frequently involve the sale of counterfeit goods on either online or physical stalls or storefronts. When authorities trace the origin of counterfeit goods, sellers typically claim to have purchased items from Mainland China’s e-commerce platforms or from unidentified wholesalers. This suggests an underlying supply chain of organized and large-scale criminal operations that provide various types of counterfeit goods to downstream distributors both domestically and internationally.

- (2) Trade secret misappropriation typically involves headhunting firms or intermediaries employed to poach and illicitly acquire confidential business information. This includes enticing employees with lucrative offers to transfer proprietary secrets upon joining competitors, establishing local branches in Taiwan to facilitate talent recruitment and information theft, engaging in economic espionage, collaborating both internally and externally to enable misappropriation, and instances wherein employees steal secrets to launch their own enterprises. Offenders leaking secrets to overseas entities may accept funds via foreign currency accounts or directly in foreign cash, both to receive payment and to obscure the act, and often possess considerable knowledge of ML.

Estimated criminal proceeds were approximately NTD2.2 billion in 2021, NTD2.3 billion in 2022, and NTD800 million in 2023.

Case Study

To conceal and obscure the origin and destination of proceeds totaling over NTD3.89 million from the sale of counterfeit goods online, Person A, acting with criminal intent, laundered money by first engaging an underground banking operator via the Internet to process the funds, subsequently using an account provided by an online auction platform to receive consumer payments. These receipts were then converted into an equivalent amount in RMB and transferred to Person A’s Alipay account in Mainland China. A subsequently engaged an unidentified mainland China individual listed as a “friend” on the Alipay to remit NT dollars from a Taiwan bank account into A’s account.

Source: Taiwan High Prosecutors Office

11. High-Risk Threat: Third-Party Money Laundering

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

The FATF defines third-party ML as the laundering of proceeds by individuals or entities not directly involved in the predicate offense. While third-party ML is not listed as a predicate offense in the FATF’s glossary of the 40 Recommendations, Taiwan’s Money Laundering Control Act prescribes criminal liability for third-party laundering. The national ML risk assessment identifies third-party ML as a significant threat, warranting separate analysis and assessment. Third-party ML involves the transfer, conversion, concealment, disguise, receipt, or possession of illicit proceeds on behalf of others. The main perpetrators generally fall into three categories: groups engaged in underground banking operations, professionals, and individual actors.

Professional third-party ML typically refers to professionals not directly involved in the predicate criminal activity, such as accountants, attorneys, and land administration agents, who possess specialized expertise and knowledge of finance, taxation, real estate, and relevant

regulations. This may also include corporate service providers or consulting firms that create complex company structures, coordinate business activities, issue fraudulent financial certifications, establish trusts, or serve as intermediaries to help offenders conceal or transfer illicit assets. In addition to professional money launderers, there are non-professionals who, driven by personal relationships or urgent financial needs, lend their bank accounts or identities to assist criminals in purchasing real estate, jewelry, or holding illicit proceeds on their behalf, despite lacking relevant expertise.

Within the scope of ML activities, professionals may utilize their regulatory knowledge to create complex company structures, arrange business operations, issue false financial certifications, establish trusts, or act as intermediaries to assist offenders in concealing or transferring illegal proceeds. All sectors that could be exploited for ML—for example, banks, securities firms, investment advisory companies, or virtual asset service providers—are potentially exposed to involvement.

Estimated criminal proceeds reached approximately NTD21.99 million in 2021, NTD23.13 million in 2022, and NTD30.64 million in 2023.

Section 2. Terrorism Financing Threats

There are no terrorist organizations operating in Taiwan, nor are there any international terrorist organizations with branches in Taiwan. From 2021 to 2023, no FT incidents occurred domestically, nor were any terrorists, terrorist organizations operating locally, or cases of financing terrorist organizations detected during this period. Taiwan assesses potential FT threats using seven indicators: the degree of direct or indirect contact between terrorist financiers and terrorist organizations; the knowledge, skills, and professionalism of terrorist financiers in carrying out FT; their networks, resources, and operational capabilities; the scope and regions accessible for terrorist financing operations; the estimated annual volume of funds raised; the range of methods employed for collecting and managing funds; and the degree to which these funds are used to harm Taiwan or international interests.

1. Degree of Direct/Indirect Contact with Terrorist Organizations

Taiwanese society is founded on democratic freedom, enriched by cultural diversity, and characterized by interfaith harmony. There has never been a terrorist attack in Taiwan, nor have international or regional terrorist organizations recruited personnel or raised funds; furthermore, no cases of Taiwanese nationals engaging in terrorist activities in conflict zones have been reported. In recent years, terrorist organizations have sought to attract public attention by disseminating violent propaganda online; however, no such cases have been observed in Taiwan over the past 3 years.

2. Knowledge, Skills, and Expertise in Terrorist Financing

Terrorist financiers might exploit Taiwan's open economic and trade environment to conduct FT activities, including fundraising independently or via front companies, fraud, using other criminal proceeds, or operating through NPOs. Funds may be moved through methods such as money or value transfer services, physically carrying cash abroad, or converting funds into virtual assets. However, no cases of terrorist financiers raising funds for terrorist activities have been identified in Taiwan.

3. Networks, Resources, and Operational Capacity

Between 2021 and 2023, no individuals or groups were found to have funded terrorists or organizations, nor was there any domestic fundraising to support terrorists or terrorist organizations. While there have previously been cases where migrant workers in Taiwan raised small amounts of funds for orphans in Middle Eastern conflict zones, no concrete evidence of FT was uncovered. Considering the limited earnings of migrant workers in Taiwan, their capacity to finance terrorist activities is considered minimal. Furthermore, networks, resources, and capabilities for identifying potential high-risk terrorists remain limited.

4. Scope and Area of Terrorist Financing Activities

Taiwan's open trade policies and favorable investment environment mean that designated sanctioned terrorist organizations, entities, or individuals may attempt to use front companies or conduct transactions with domestic companies through third-party jurisdictions to circumvent sanctions. However, to date, no cases of cross-border FT have been identified in Taiwan.

Based on geographical analysis and foreign population composition, cross-border salary remittances from Taiwan are predominantly sent to Indonesia and Vietnam. Therefore, the operational scope and area for potential terrorist financing activities are concentrated in Southeast Asian countries, such as Indonesia, Vietnam, the Philippines, Thailand, and Malaysia, with the overall range of FT capabilities remaining relatively limited.

5. Estimated Annual Amount of Terrorist Financing

From 2021 to 2023, Taiwan did not detect any terrorist attacks or FT cases; accordingly, there are no estimated amounts for FT during this period.

6. Diverse Methods Used by Terrorist Financiers to Collect and Manage Funds

No cases have been found of individuals or groups providing financial support to terrorists or terrorist organizations in Taiwan, nor have any suspicious fundraising platforms been identified. Should any potential terrorist financiers exist, their collection and handling of funds would likely be limited to traditional channels. If new means, such as virtual assets or other emerging transaction methods, are employed, Taiwan has implemented relevant supervisory measures to monitor and detect unusual fund flows; however, no related cases have been reported in the past 3 years.

7. Extent to Which Raised Funds Are Used to Harm Taiwan or International Interests

At present, Taiwan has no cases of FT, making it difficult to assess the immediacy or degree of harm such activities could cause. As a result, the impact or damage that potential offenses and FT activities may have on the financial system, institutions, economy, or society cannot be evaluated at this time.

Chapter 6. Risk Assessment Results: Money Laundering and Terrorist Financing Vulnerabilities

Section 1 National Assessment Results for ML/FT Vulnerabilities

1. Government Organization and Judicial Structure

Taiwan is a constitutional democracy with a governmental structure divided into the central/municipal, county (city), and township (town, city) levels. The central government comprises the Office of the President and five branches: the Executive Yuan, Legislative Yuan, Judicial Yuan, Examination Yuan, and Control Yuan.

The Constitution serves as Taiwan's fundamental law and holds the highest legal authority—no law, regulation, or decree may contravene it. The Constitution defines the organization of the state and the fundamental rights and duties of the people. Regarding national organization, it establishes a separation of five branches within the central government and a system of local self-government, explicitly ensuring a balance of powers between central and local authorities while outlining basic national policies. With regard to citizens' rights, it enshrines the principle of popular sovereignty and guarantees fundamental rights for all people. In accordance with the Constitution, the President and Vice President are directly elected by the entire electorate to serve 4-year terms and may be re-elected once. The President is the head of state; represents the country externally; commands the land, sea, and air armed forces; promulgates laws and issues orders according to the law; can declare martial law; and appoints or removes civil and military officials.

The Executive Yuan is the highest administrative organ of the country, comprising 14 ministries and 17 other agencies of equivalent rank. The Legislative Yuan is the nation's highest legislative body, composed of legislators elected by the people, each serving a 4-year term with the possibility of indefinite re-election. The Judicial Yuan is the highest judicial authority that houses the Constitutional Court; it is composed of justices who adjudicate cases involving constitutional review of statutes and judgments, disputes among government agencies, impeachment of the President and Vice President, dissolution of unconstitutional political parties, protection of local self-government, and uniform interpretation of laws and orders. The courts at all levels under the Judicial Yuan are responsible for adjudicating civil, criminal, administrative litigation, and disciplinary cases involving public officials. Unlike most countries that follow the tripartite separation of powers, Taiwan adopts a unique five-branch system. Among these, the Examination Yuan serves as the highest examination authority, overseeing civil service examinations, personnel management, and the appointment and removal of civil servants. The Control Yuan is the highest supervisory body, exercising powers of impeachment, censure, and audit.

Taiwan's judicial system is founded on the civil law tradition, where abstract, codified statutes form the primary legal framework. Judges at all levels are required to render decisions independently in accordance with the law. Since July 2019, for cases before the Supreme Court involving divergent interpretations or significant fundamental legal questions, Taiwan has implemented the Grand Chamber mechanism to unify legal interpretations, replacing the prior system of binding precedents and resolutions. Taiwan's judicial system is structured as a

three-instance system: district courts are generally responsible for first-instance trials; the High Court and its branches handle appeals against first-instance judgments; and the Supreme Court, as the court of last resort, conducts reviews solely on matters of law, differing from the fact-finding role of the lower courts. The prosecution system is also organized into three levels to correspond with the court system: the Supreme Prosecutors Office, High Prosecutors Office and its branches, and the district prosecutors offices. Under the principle of prosecutorial unity, the Prosecutor General of the Supreme Prosecutors Office lawfully directs and supervises prosecutors at all levels in conducting criminal investigations, filing and carrying out public prosecutions, assisting or acting in private prosecutions, overseeing the execution of criminal judgments, and performing other duties as specified by law. Additionally, the Citizen Judges Act was enforced on January 1, 2023, to achieve citizen participation in the judiciary, enhance judicial transparency, reflect the public's sense of justice, and highlight the concept of popular sovereignty. By participating in trials, citizens gain a thorough understanding of how judges establish facts, interpret the law, and determine sentences. In turn, courts enrich their adjudication through this dialogue with the public, broadening both perspective and substance.

Since the government's relocation from Mainland China to Taiwan in 1949—and especially after the lifting of martial law in 1987—Taiwan has developed within a stable and robust democratic environment, with separation of powers among the five branches and multiple peaceful transfers of political power, resulting in a mature democratic society and a capable, honest government. According to “Freedom in the World” published by the U.S.-based NGO Freedom House—a widely recognized benchmark for assessing global democracy, freedom, and human rights—Taiwan achieved a score of 94 out of 100, earning the rating of “Freest.” Additionally, in the 2023 Corruption Perceptions Index released by Transparency International, Taiwan ranked 28th among 180 countries worldwide, placing it within the top 15% globally and demonstrating Taiwan's effective anti-corruption efforts.

While these laws and agencies play a critical role in combating crime, the freedom afforded to Taiwanese citizens and the legal and procedural safeguards designed to protect defendants may also be exploited by criminals, including money launderers and terrorist financiers.

2. Geographical Location

Taiwan is situated in East Asia, between southeastern Mainland China and the western Pacific. To the north lie Japan's Ryukyu Islands, to the south the Philippine Islands, and to the west Mainland China, forming a long, narrow island. Taiwan stretches approximately 395 kilometers from north to south and has a maximum east-west width of about 144 kilometers, covering an area of approximately 36,000 square kilometers (about 14,400 square miles). Taiwan's advantageous geographic position has made it a transportation hub in East Asia.

Due to its location, Taiwan is susceptible to cross-border criminal activities, especially those exploiting air and sea transportation routes, which pose significant challenges to detection and enforcement. Taiwan's neighboring regions include North Korea—a high-risk jurisdiction designated by the FATF; mainland China, an international economic powerhouse; and Hong Kong, a key financial center in the Asia-Pacific. In recent years, this factor has had a growing impact on the risks of ML and FT in Taiwan.

3. Economic and Trade Environment

According to IMF estimates of global gross domestic product (GDP) for 2022, Taiwan, with a total value of USD760.5 billion, surpassed Sweden, Belgium, and other countries to become the world's 21st-largest economy. Riding the global economic growth trend, Taiwan has also experienced significant economic expansion. Taiwan's annual per capita GDP surpassed USD30,000 for the first time in 2021, indicating the country's resilient and robust economic performance⁷. In terms of industrial structure by sector, Taiwan's GDP incorporates agriculture, forestry, fishing, animal husbandry, industry, and services. Industry accounts for approximately 36.38% of Taiwan's GDP, with manufacturing constituting the largest share at 32.56%. The services sector accounts for 61.03% of the GDP, with wholesale and retail trade contributing 15.39% and the financial and insurance sector accounting for 6.40%. The shares of other sectors are as follows⁸.

| Industry | GDP Share in 2023 |
|---|-------------------|
| Agriculture, Forestry, and Fishing | 1.47% |
| Industry – Mining and Quarrying | 0.05% |
| Industry – Manufacturing | 32.56% |
| Industry – Electricity and Gas Supply | 0.12% |
| Industry – Water Supply and Pollution Remediation | 0.53% |
| Industry – Construction | 3.12% |
| Services – Wholesale and Retail Trade | 15.39% |
| Services – Transportation and Storage | 3.19% |
| Services – Information and Communications | 3.26% |
| Services – Financial and Insurance | 6.40% |
| Services – Real Estate | 7.74% |
| Others | 25.05% |

Taiwan has an export-oriented economy, where trade serves not only as the lifeblood of economic development but also as a vital conduit for global connectivity. As of the end of 2023, Taiwan's trade dependency ratio reached 108.33%. Its total trade volume amounted to USD784.4 billion, with export orders totaling USD517.2 billion. The top three export categories by value were electronic components (41.32%), information and communication and audiovisual products (19.27%), and basic metal products (6.65%). The top three import

⁷ Source: <https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvNzE2NS8zNzc-1Ny84YzQ3NmM3OC00MjllLTQ2MDQtOWEwMC1kNzdhMGQ0OTc0NGEucGRm&n=5pS%2f5bqc57aT5r%2bf55m85bGV5oiQ5p6c5Zue6aGn6liH5pyq5L6G57aT5r%2bf5oOF5Yui5bGV5pybXzIwMjQwMTA15pu05pawLnBkZg%3d&icon=.pdf> (Last accessed November 12, 2024)

⁸ Source: <https://dmz26.moea.gov.tw/GA/common/Common.aspx?code=A&no=6> (Last accessed November 12, 2024)

categories were electronic components (23.13%), mineral products (17.64%), and machinery (10.64%). In 2023, Taiwan's largest export market was Mainland China (including Hong Kong), accounting for 35.2% of total exports. The ASEAN-10 countries ranked second with 17.64%, followed closely by the United States at 17.63%. Exports to Japan and the European Union accounted for 7.27% and 8.51%, respectively. In the same year, the primary source of imports was Mainland China (including Hong Kong), accounting for 30.37% of total imports. Japan was the second-largest source, at 12.59%; the ASEAN-10 countries accounted for 11.66%, United States made up 11.56%, and Europe comprised 10.53%⁹ of Taiwan's total imports. Taiwan's thriving import–export trade involves cross-border financial flows, and its traded goods may also involve high-risk jurisdictions, thereby increasing the risks of ML and FT.

The types of legal persons in Taiwan are mainly categorized as associations (including public-benefit and for-profit associations) and foundations. As of the end of 2023, the total number of registered for-profit entities, namely companies, reached 771,311. Limited companies (578,810) comprised the majority, followed by companies limited by shares (186,836). There were 2,641 public companies and 184,195 non-public companies (including 5,434 closed companies). As for NPOs, these include people's organizations and foundations, which are overseen by the Ministry of the Interior, the Ministry of Health and Welfare, the Ministry of Education, the Ministry of Culture, and municipal or county governments. By the end of 2023, the total number of nationwide NPOs was approximately 20,000, comprising categories such as people's organizations, nationwide religious organizations, social welfare organizations, medical organizations, educational organizations, and cultural organizations.

Its open and stable economy, coupled with advanced global trade networks, presents opportunities that may be exploited by domestic and foreign criminal actors, money launderers, and terrorist financiers alike. Due to Taiwan's high economic and trade dependency, cross-border financial flows, and the risk that imported and exported goods may involve high-risk jurisdictions, the economic environment may also indirectly affect the development of the underground economy. Accordingly, Taiwan has established comprehensive and effective measures in its legal, supervisory, and law enforcement frameworks and has promoted close cooperation between supervisory and law enforcement authorities to effectively mitigate the risks of ML, FT, and PF.

4. Financial System

Taiwan's financial system is mature and diversified, playing a significant role in the national economy. As of the end of 2023, total assets of the financial system amounted to approximately 504.73% of the GDP, while the output of the financial and insurance sector accounted for about 6.40% of Taiwan's GDP. Among the financial industries in Taiwan, domestic banks comprise the largest sector based on total assets, accounting for 50.32% of the financial industry's assets. The second-largest are life insurance companies, whose total assets comprise 29.37% of the industry. Because domestic banks provide a wide range of services—including deposit accounts (featuring cash payments and monetary instruments), remittance services (domestic and cross-border fund transfer services), and trade financing—they form the most important sector within Taiwan's financial industry. Since 2021, the Financial Supervisory Commission

⁹ Source:
https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=1374&pid=776523&dl_DateRange=all&txt_SD=&txt_ED=&txt_Keyword=&pageindex=1&history (Last accessed November 12, 2024)

has approved qualified companies to operate “foreign migrant worker cross-border small remittance” services. As this service is restricted, clients must be foreign migrant workers, the remittance amount and source of funds are both limited, and the companies are relatively small in terms of assets, placing them in the small-scale financial services industry. Other types of financial industries in Taiwan are detailed below.

Reference Date: End of December 2023

| Type | Number of Institutions | Number of Domestic Branches (Including Head Offices) | Total Assets (NTD billion) | Percentage of Total Financial Industry Assets (%) | Share of 2023 GDP (%) |
|--|------------------------|--|----------------------------|---|-----------------------|
| Domestic Banks | 38 | 3,431 | 598,800 | 50.32% | 253.98% |
| Foreign Bank Branches in Taiwan | 31 | 40 | 55,400 | 4.91% | 24.80% |
| Postal Institutions | 1 | 1,297 | 83,317 | 7.01% | 35.39% |
| Agricultural FIs (including the National Agricultural Finance Corp. and Farmers’ and Fishermen’s Credit Departments) | 312 | 1,160 | 35,951 | 3.03% | 15.27% |
| Electronic Payment Institutions | 10 | 10 | 399 | 0.03% | 0.17% |
| Credit Unions | 23 | 312 | 9,330 | 0.79% | 3.96% |
| Foreign Migrant Worker Remittance Companies | 3 | 3 | 33 | 0.00% | 0.01% |
| Financial Leasing Businesses | 19 | 134 | 10,333 | 0.87% | 4.39% |
| Bills Finance Companies | 8 | 38 | 11,212 | 0.94% | 4.76% |
| Credit Card Companies | 4 | 4 | 66 | 0.01% | 0.03% |
| Life Insurance Companies | 26 | 142 | 349,033 | 29.37% | 148.24% |
| Insurance Agent and Broker Companies | 566 | 566 | 65 | 0.01% | 0.03% |
| Non-Life Insurance Companies | 22 | 179 | 4,759 | 0.40% | 2.02% |
| Virtual Asset Service Providers | 25 | 25 | 57 | 0.00% | 0.02% |
| Securities Firms | 65 | 811 | 25,453 | 2.14% | 10.81% |
| Securities Investment Trust Enterprises (including Futures Trust Enterprises) | 38 | 80 | 757 | 0.06% | 0.32% |

| | | | | | |
|--|-------|-------|-----------|---------|---------|
| Securities Finance Enterprises | 1 | 3 | 576 | 0.05% | 0.24% |
| Futures Commission Merchants (including Managed Futures Enterprises and Leveraged Transaction Merchants) | 15 | 31 | 657 | 0.06% | 0.28% |
| Total | 1,207 | 8,266 | 1,188,398 | 100.00% | 504.73% |

Source: Financial Supervisory Commission (FSC); Ministry of Agriculture (MOA)

In March 2023, the Financial Supervisory Commission was designated as the competent authority for overseeing virtual asset service providers engaged in financial investment or payment-related activities. Although this sector is generally small in scale, virtual assets are transacted online, enabling the rapid transfer of large sums and allowing for cross-border transfers; this facilitates the use of virtual assets by criminal organizations as channels for ML. In summary, Taiwan offers diverse financial products and services and, through its highly developed financial system, manages and intermediates substantial volumes of funds from various sources.

To enhance Taiwan's AML/CFT/CPF regime, all DNFBPs, as defined by the FATF, have been brought under the Money Laundering Control Act, with corresponding competent authorities for each industry responsible for establishing regulations and supervising compliance with AML/CFT/CPF obligations. The following table provides an overview of Taiwan's DNFBPs as of the end of 2023.

Reference date: Except for attorneys, the data are as of the end of 2022;
for all other categories, the data are as of the end of December 2023.

| Industry | Number of Approved Operating Entities | Number of Employees |
|--|---------------------------------------|---------------------|
| Certified Public Accountants | 2,284 | 4,004 |
| Jewelry Businesses | 4,672 | |
| Attorneys | 4,078 | 11,998 |
| Businesses or Individuals Providing Third-Party Payment Services | 53 | |
| Real Estate Brokerages | 8,718 | |
| Land Administration Agents | | 10,422 |
| Bookkeepers and Tax Agents | | 9,173 |
| Notaries | 220 | 266 |

Source: Securities and Futures Bureau of the Financial Supervisory Commission, Department of Commerce of the Ministry of Economic Affairs, Department of Land Administration of the Ministry of the Interior, Prosecutors Office of the Ministry of Justice, Civil Department of the Judicial Yuan, Taxation Administration of the Ministry of Finance, Administration for Digital Industries of the Ministry of Digital Affairs

To optimize the development environment for businesses or individuals providing third-party payment services in Taiwan, the Digital Industries Administration of the Ministry of Digital Affairs, as the competent authority, has specifically planned to establish a service capability registration mechanism for third-party payment service providers. This mechanism aims to inventory the domestic third-party payment service capacity through a credible registration platform, construct an industry map for the sector, expand the scale and scope of industry services, accelerate and enhance industry value and competitiveness, and ensure compliance with AML obligations¹⁰.

The United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA) pointed out in April 2013 that "financial inclusion is a driver or accelerator of economic growth, job creation, and social development." As a result, Taiwan's financial supervisory authorities have continued to help narrow the wealth gap, enhance social equity, and support inclusive economic growth¹¹. For 2023, Taiwan's financial inclusion measurement results indicate that there are 17 commercial bank branches per 100,000 adults, surpassing the global average of 15.9 branches per 100,000 adults¹². The number of automated teller machines (ATMs) per 100,000 adults is 168, also higher than the global average of 51.2¹³. The account ownership rate among adults is 92.1%¹⁴, higher than the global average of 76.2%¹⁵. With the ongoing development of e-commerce and digitalization, digital finance has advanced significantly in Taiwan over the past few years. The number of mobile payment transactions per 100,000 adults reached 4,239,956, surpassing the global average of 4,233,047.¹⁶ Additionally, 95.5% of adults¹⁷ use electronic payments, which is higher than the global average of 64%¹⁸.

Payment activities are deeply intertwined with the daily lives of the people of Taiwan. To ensure the smooth transfer of funds, Taiwan has established robust, comprehensive, and

¹⁰ Source: <https://moda.gov.tw/ADI/services/apply-services/energy/5757> (Last accessed November 12, 2024)

¹¹ Source: <https://www.fsc.gov.tw/ch/home.jsp?id=642&parentpath=0,7> (Last accessed November 12, 2024)

¹² Source:
https://www.fsc.gov.tw/userfiles/file/%E9%99%84%E4%BB%B6_112%E5%B9%B4%E6%9C%AC%E6%9C%83%E6%99%AE%E6%83%A0%E9%87%91%E8%9E%8D%E8%A1%A1%E9%87%8F%E5%8F%8A%E8%A7%80%E5%AF%9F%E6%8C%87%E6%A8%99%E8%A1%A1%E9%87%8F%E7%B5%90%E6%9E%9C.pdf (Last accessed November 12, 2024)

¹³ Source:
https://www.fsc.gov.tw/userfiles/nle/%E9%99%84%E4%BB%B6_112%E5%B9%B4%E6%9C%AC%E6%9C%83%E6%99%AE%E6%83%A0%E9%87%91%E8%9E%8D%E8%A1%A1%E9%87%8F%E5%8F%8A%E8%A7%80%E5%AF%9F%E6%8C%87%E6%A8%99%E8%A1%A1%E9%87%8F%E7%B5%90%E6%9E%9C.pdf (Last accessed November 12, 2024)

¹⁴ This rate refers to the proportion of the population aged 20 and above in Taiwan who hold accounts at banks, post offices, credit cooperatives, and the credit departments of Department of Farmers' Service and of Fisheries Agency. (Source: Taiwan Academy of Banking and Finance, Biennial "2022 Taiwan Financial Life Survey")

¹⁵ Source:
https://www.fsc.gov.tw/userfiles/nle/%E9%99%84%E4%BB%B6_112%E5%B9%B4%E6%9C%AC%E6%9C%83%E6%99%AE%E6%83%A0%E9%87%91%E8%9E%8D%E8%A1%A1%E9%87%8F%E5%8F%8A%E8%A7%80%E5%AF%9F%E6%8C%87%E6%A8%99%E8%A1%A1%E9%87%8F%E7%B5%90%E6%9E%9C.pdf (Last accessed November 12, 2024)

¹⁶ Source:
https://www.fsc.gov.tw/userfiles/nle/%E9%99%84%E4%BB%B6_112%E5%B9%B4%E6%9C%AC%E6%9C%83%E6%99%AE%E6%83%A0%E9%87%91%E8%9E%8D%E8%A1%A1%E9%87%8F%E5%8F%8A%E8%A7%80%E5%AF%9F%E6%8C%87%E6%A8%99%E8%A1%A1%E9%87%8F%E7%B5%90%E6%9E%9C.pdf (Last accessed November 12, 2024)

¹⁷ Adults aged 18 and above in Taiwan (Source: Taiwan Academy of Banking and Finance, Electronic Payment Network Survey)

¹⁸ Source: <https://www.fsc.gov.tw/ch/home.jsp?id=838&parentpath=0,7> (Last accessed November 12, 2024)

digitally responsive payment infrastructure to address the challenges presented by modern e-commerce and digitalization. The Central Bank Interbank Funds Settlement System (CIFS) connects key domestic payment and settlement systems, handling the final settlement of large-value payments¹⁹, retail payments²⁰, and financial market transactions. Regarding large-value payments, in 2023, CIFS processed transactions totaling NTD547 trillion—approximately 23 times the nation’s GDP for the year—covering around 753,000 transactions, with those exceeding NTD10 million each accounting for about 85.8% of the total.

For retail payments, while the transaction value is generally lower than that of the large-value payment system, the transaction volume is much higher. The Interbank Financial Information System processed 1.28 billion retail payment transactions in 2023, surpassing the 753,000 transactions processed by CIFS in the same year, with a transaction value of NTD20.2 trillion. Retail payments encompass a wide variety of transactions, including remittances, transfers, withdrawals, bill payments, and tax payments. The primary retail payment instruments in Taiwan include cash, checks, debit cards, credit cards, deposit account transfers, direct debit, and electronic money (such as stored-value cards and electronic payment accounts).

As of the end of 2023, the amount of currency in circulation (i.e., cash held by the public) was approximately NTD3.1 trillion. Due to its anonymity, cash remains a preferred tool for ML among criminal organizations. For non-cash payment instruments, both the transaction value and volume have increased from NTD172 trillion and 4.88 billion transactions in 2018 to NTD221.4 trillion and 7.51 billion transactions in 2023, respectively. Transfers made through deposit accounts constitute approximately 90.3% of the total transaction value in non-cash payments, while electronic money transactions constitute only 0.2% of the total transaction volume. With the increasing prevalence of mobile network, the mobile payment²¹ industry has experienced rapid growth. According to a survey conducted by the Institute for Information Industry, regular use²² of mobile payments increased from 52.8% in 2019 to 70.6%²³ in 2022. This indicates that Taiwan’s diversified payment instruments can meet the payment needs of the public in various transaction scenarios.

Moreover, with recent technological innovation, some residents have begun using virtual assets for payments. Although these assets are not issued by central banks, depository institutions, or electronic money institutions—and do not carry legal tender status—they hold transactional value, enable cross-border transfers, support rapid exchanges, and operate on decentralized systems. These characteristics make them vulnerable to exploitation by illicit actors for speculation and unlawful transactions. In September 2023, the Financial Supervisory Commission issued the “Guidelines for the Management of Virtual Asset Service Providers (VASPs),” which references international supervisory trends and gradually enhances the protection of customer rights and the safety of financial transactions by domestic virtual asset service providers.

¹⁹ Primarily processes transactions between financial institutions and those related to financial market activities.

²⁰ Handles payments made by individuals or businesses.

²¹ Mobile payment generally refers to the act of making payments by binding payment instruments (e.g., credit cards, debit cards, and electronic payment accounts) to mobile devices.

²² The popularity of mobile payments is based on a survey conducted by the Institute for Information Industry (III), which sampled consumers’ preferences for four payment instruments, allowing for multiple responses.

²³ Source: <https://www.cbc.gov.tw/public/data/data/payandsettlementsys112.pdf> (Last accessed: November 12, 2024)

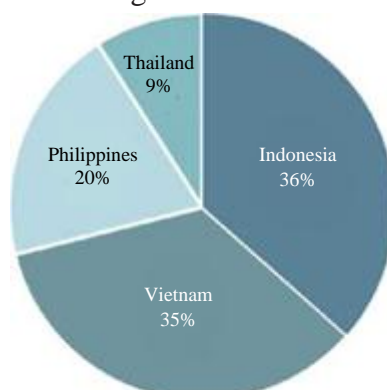
In summary, Taiwan already possesses a sound financial infrastructure, and all types of financial institutions provide a diverse array of payment services. Large-value payments are primarily processed electronically, while retail payments can be made using cash and various convenient electronic payment instruments. Taiwan continues to promote the development of a user-friendly mobile payment environment, in collaboration with the information and communications security industry, which helps reduce reliance on cash transactions and mitigate associated risks related to ML and FT. In addition, due to the decentralized and cross-border transfer characteristics inherent to virtual assets, they are prone to being used as tools for ML and FT. Consequently, Taiwan has already adopted corresponding policies and regulations to mitigate the occurrence of ML/FT risks.

5. Population Structure

Taiwan has a population of approximately 23 million people, which includes the Indigenous peoples who have been living in Taiwan for generations, accounting for approximately 2.36% of the total population. The rest comprises the Han people, who migrated to Taiwan after the 17th century. The integration of various ethnic groups has shaped Taiwan's rich cultural landscape. This diversity is prominently reflected in religious beliefs, architectural styles, languages, everyday customs, and culinary traditions, all of which contribute to a harmonious and vibrant multicultural society. About 70% of Taiwan's population is concentrated in the five major metropolitan areas in the western region (Taipei, Taoyuan, Taichung, Tainan, and Kaohsiung), with the largest concentration being in the Taipei metropolitan area—where both the capital, Taipei City, and the largest city, New Taipei City, are located.

As of the end of December 2023, the number of foreign nationals holding residency permits in Taiwan—including civil and business personnel, doctors, engineers, missionaries, workers in construction and manufacturing, caregivers and domestic helpers, students, and family members—stood at approximately 974,000, with the top five nationalities all from Southeast Asian countries, together accounting for 90.5%: Indonesia (30.5%), Vietnam (29.9%), the Philippines (18%), Thailand (9.3%), and Malaysia (2.85%). In addition, the vast majority of the 753,000 migrant workers in Taiwan are from Southeast Asian countries: Indonesia (36.22%), Vietnam (34.94%), the Philippines (19.83%), and Thailand (9.02%)²⁴.

Taiwan migrant worker shares:



²⁴ Source: National Immigration Agency, Ministry of Interior; Ministry of Labor

6. Consequences of Money Laundering and Terrorist Financing

International experience in AML/CFT shows that major offenders frequently use money laundering channels to “cleanse” illicit funds, thereby legitimizing their criminal earnings and evading law enforcement or even reinvesting criminal proceeds in further criminal acts.

ML has far-reaching effects on both the economy and society. When major offenders accumulate substantial profits and wealth, they can infiltrate and corrupt government institutions, legitimate businesses, and financial systems, as well as influence various levels of society.

Moreover, ML allows criminals to preserve and increase their illicit gains, making any country or region that serves as a laundering haven a magnet for more criminal actors. This, in turn, fosters the growth of organized crime, corruption, bribery, drug trafficking, fraud, and other related offenses. In addition to imposing substantial social costs on crime control efforts, ML distorts national policies, harms a country’s reputation and economic stability, reduces tax revenues, hinders international investment, disrupts the overseas expansion of legitimate enterprises, and significantly undermines the credibility and stability of financial institutions. Such damage can even undermine social fairness and justice. Failure to adequately comply with international AML standards may result in the country being subject to international sanctions.

For example, some of the most severe harm suffered by the people of Taiwan is caused by fraud rings and high-yield investment schemes. These groups not only deceive local citizens but have also extended their operations overseas, causing significant damage to the country’s reputation. After illicit proceeds are transferred to front accounts, they may be withdrawn domestically by cash couriers or, after being moved through multiple accounts, be converted into virtual asset accounts and laundered overseas, making recovery exceedingly difficult. If there are gaps in a country’s AML defenses, the overall order of financial flows will be disrupted, which may prompt other countries to impose sanctions or blockades, thereby affecting legitimate financial transactions.

In recent years, rapid technological advancements have diversified methods of fund transfer, with many exploiting the unregulated nature of internet-based platforms. This has facilitated easier movement of funds while simultaneously complicating efforts to combat ML and counter FT. The challenges that emerging technologies pose to AML/CFT efforts will continue to be a priority for future initiatives.

Section 2. Assessment Results of the Industry/Sector ML/FT Vulnerabilities

In this risk assessment, a total of 36 sectors/industry types in Taiwan were evaluated. Each was assessed according to their inherent characteristics, the nature of their products and services, the nature of their business relationships with clients, the geographic scope of their operations, and the nature of their service delivery channels.

Compared with the previous assessment, this cycle introduced “foreign migrant worker remittance companies” as a new evaluation item. In addition, to enable more effective allocation of supervisory resources, “futures trust enterprises” have now been included in the joint assessment with “securities investment trust enterprises,” forming a combined category “securities investment trust enterprises (including futures trust enterprises).” Similarly, “managed futures enterprises” and “leverage transaction merchants” were grouped together under “futures commission merchants (including managed futures enterprises and leverage transaction merchants)” for a unified evaluation.

With respect to control effectiveness and residual risk assessment incorporated in this review, actual implementation of AML and CFT controls varies by industry/sector, but the overall approaches to control are similar. The following highlights the control measures implemented in each industry/sector to assist users in understanding how risks are managed. As for the actual assessment results, as they involve sensitive details of supervisory measures, the identification results are intended for reference by public sector agencies.

I. Risk Assessment

- (1) Periodically conduct comprehensive risk assessments that cover customers, products/services, channels, and geographic factors and apply enhanced measures to address high-risk circumstances.
- (2) Fully consider risk factors related to customers, products/services, channels, and geographic factors and establish individual customer risk profiles.
- (3) Prior to launching any new product or service, conduct an assessment of ML/FT risks relevant to that product or service.

II. Customer Due Diligence

- (1) Use reliable identification data to verify customer identities and collect adequate information to understand the nature and purpose of each customer's business activities.
- (2) Understand the customer's ownership and control structure and use reliable identification data to identify and verify the beneficial owner of the customer.
- (3) Conduct CDD in line with the customer's risk profile and perform ongoing due diligence regularly or when trigger events occur to ensure that customer and business information remains current and timely.
- (4) For situations presenting high ML/FT risk, conduct enhanced due diligence measures commensurate with the risk level and obtain appropriate senior management approval prior to establishing or maintaining a business relationship with high-risk customers.
- (5) Maintain accurate records of CDD, account documentation, business relationship records, and transaction records and be able to promptly provide such records upon request of competent authorities.

III. Suspicious Transaction Reporting for ML/FT and Targeted Financial Sanctions

- (1) Criteria and systems based on rule-based and scenario-based approaches must be established to detect unusual transactions and to verify whether transactions executed by customers align with the institution's risk-based understanding of the customer and their business.
- (2) The system for identifying unusual transactions is appropriately calibrated, and institution staff are able to effectively process alerts generated by the system.
- (3) Suspicious transaction reports (STRs) must contain information of value to the Financial Intelligence Unit (FIU) and their submission must comply with regulatory timeliness requirements.

- (4) Before establishing a business relationship with a customer, during the course of the relationship, and before the completion of a transaction, automated sanctions list screening using fuzzy matching must be performed on the customer and related parties.
- (5) Such automated sanctions list screening using fuzzy matching must be conducted on the customer and related parties within a reasonable timeframe following updates to sanctions lists, changes in customer-related information, or the occurrence of trigger events.
- (6) Automated system calibration results and rule/scenario settings must be regularly reviewed to ensure effective operation of the system.
- (7) Investigation procedures must be in place to determine whether an alert is a true match or a false positive and appropriate controls must be implemented for true matches.
- (8) Clear audit trails must be maintained to document judgments regarding unusual transactions, potential matches with blacklists, and the corresponding measures taken.

IV. Internal Controls

- (1) Develop and implement AML/CFT policies and procedures commensurate with the institution's scale and risk level, ensuring that both management and employees understand and execute related policies and procedures.
- (2) Have sufficient resources dedicated to AML/CFT compliance functions, appoint senior management to supervise, and ensure appropriate access to internal documents and direct reporting to the institution's management.
- (3) Develop and implement AML/CFT training programs to provide adequate training for relevant personnel.
- (4) Ensure that the responsibility and authority for suspicious transaction reporting rest with compliance staff and are not subject to interference from other business units or senior management.
- (5) Maintain an independent internal audit function to assess the institution's compliance with AML/CFT requirements and report audit findings and related recommendations directly to the Board of Directors.
- (6) Appoint external auditors to ensure that the institution complies with AML/CFT requirements.
- (7) Implement group-wide AML/CFT policies and procedures, including information sharing for AML/CFT purposes and protection measures to maintain the confidentiality of exchanged information.
- (8) Maintain a group-level compliance function, cooperating and conducting information exchanges among group members for AML/CFT purposes.
- (9) Have a group-level audit function in place.

To assist users in prioritizing resource allocation toward higher-risk and emerging sectors, as well as developing appropriate risk-mitigation measures, this section discloses the fifteen sectors identified as possessing very high and high vulnerabilities in the current or previous assessments, along with one newly assessed sector.

The table below summarizes ML/FT vulnerability identification results by industry/sector.

| Industry/sector Vulnerability Rating Table | | | |
|--|--|---|---|
| Low | Medium | High | Very High |
| 1. Pawnshop Sector 2. Foreign Currency Exchange Business 3. Centralized Securities Depository Enterprise | 1. Online Gaming Business 2. Securities Investment Trust Enterprises (including Futures Trust Enterprises) 3. Electronic Payment Institutions 4. Automotive Dealerships 5. Art Auction Houses 6. Securities Investment Consulting Enterprises 7. Land Administration Agents 8. Securities Finance 9. Futures Commission Merchants (including Managed Futures Enterprises and Leverage Transaction Merchants) 10. Foreign Migrant Worker Remittance Companies (newly added) 11. Credit Cooperatives 12. Financial Leasing Business 13. Insurance Agents and Broker Companies 14. Bookkeepers and Tax Agents 15. Bills Finance Companies 16. Notaries Public 17. Credit Card Companies 18. Non-Life Insurance Companies | 1. International Securities Branch (OSU) 2. Foreign Bank Branches in Taiwan 3. Offshore Insurance Unit (OIU) 4. Securities Firms 5. Jewelry Dealers 6. Postal Institutions Handling Savings and Remittances 7. Life Insurance Companies 8. Certified Public Accountants 9. Attorneys 10. Enterprises or Persons Providing Third-Party Payment Services 11. Real Estate Brokerage 12. Agricultural Financial Institutions (including Agricultural Bank of Taiwan, Credit Departments of Farmers' and Fishermen's Association) | 1. Offshore Banking Unit (OBU) 2. Enterprises or Persons Providing Virtual Asset Services (Virtual Asset Service Providers) 3. Domestic Banks |

1. Very High-Risk Vulnerability: Offshore Banking Units

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

OBU are established by domestic banks and branches of foreign banks with a presence in Taiwan subject to approval under the law, with each bank eligible to apply for the establishment of one OBU. As of the end of December 2023, a total of 59 banks (including 35 domestic banks and 24 branches of foreign banks in Taiwan) had established OBUs. At the end of December 2023, the total assets of all OBUs amounted to NTD7.99 trillion. Total deposits were NTD3.48 trillion, with pre-tax profit of NTD56.26 billion, reflecting significant

sector scale. In December 2023, the total amount of inward remittances for OBUs was approximately NTD24.4 trillion and outward remittances were around NTD26.5 trillion, both indicating substantial transaction volume.

OBUs are permitted to conduct a wide range of businesses, including foreign currency deposits; foreign currency lending; the sale of foreign currency financial bonds; brokerage, intermediary, and agency services for the trading of foreign currency securities and financial products; issuance, advising, negotiation, and collection of foreign currency letters of credit; foreign currency remittances; foreign exchange transactions; the underwriting of offshore securities; advisory services for asset allocation or financial planning; and various trust businesses in foreign currencies. Among these, services such as foreign currency deposits, trade finance, foreign currency remittances, and foreign exchange transactions present significant ML and FT vulnerabilities. Pursuant to Article 7 of the Offshore Banking Act, OBUs are prohibited from accepting foreign currency cash and may not exchange foreign currency deposits for NTD cash. Therefore, OBUs do not provide products or services involving cash payments or monetary instruments and are thus exempt from the large-value cash transaction reporting requirements under Article 13 of the Regulations Governing Anti-Money Laundering of Financial Institutions.

The business relationships between OBUs and their clients are predominantly offshore and highly complex in nature. Some intermediary services involve indirect relationships with clients, which can result in significant ML/FT vulnerabilities. Most OBU customers are primarily offshore legal persons, accounting for over 96% of the total client base. In 2023, among OBU individual clients, high-risk customers accounted for approximately 77.23% of active clients, while clients with assets under management exceeding USD1 million (or the equivalent in NTD) comprised approximately 1.95%. For OBU corporate clients in 2023, high-risk customers represented about 45.81% of all clients that year, and corporate customers with ownership structures comprising more than two layers accounted for approximately 6.52%.

Most OBU business relationships are predominantly with Taiwan businesses registered offshore. According to statistics, the top five jurisdictions for corporate client registration are the British Virgin Islands, Samoa, Hong Kong, Seychelles, and Belize. In 2023, the share of OBU inward and outward remittances involving high-risk jurisdictions was not high.

OBUs provide clients with online banking and other non-face-to-face transaction services, which have increasingly become the primary channels for conducting business operations. In 2023, non-face-to-face transactions accounted for approximately 53.14% of all OBU outward transactions (including face-to-face and non-face-to-face transactions). OBUs may conduct cross-border remittance operations through correspondent banks abroad, provided that all required originator and beneficiary information is obtained in accordance with regulations. In 2023, cross-border inward remittances accounted for approximately 70.23% of all inward transfers, while cross-border outward remittances comprised about 62.85% of all outward transfers, underscoring the high-risk nature of these transaction channels.

In summary, the OBU sector is substantial in scale and offers a range of services—including foreign currency deposits, trade finance, foreign remittances, and foreign exchange transactions—that are highly susceptible to ML and FT risks. OBU transactions are predominantly offshore and highly complex, often involving high-risk jurisdictions. Additionally, non-face-to-face transactions are increasingly serving as the main channel for service delivery. Therefore, the overall risk rating for OBUs is “very high”.

2. Very High-Risk Vulnerability: Enterprises or Persons Providing Virtual Asset Services (VASPs)

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

According to the FATF definition, a VASP refers to any natural or legal person who, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person.

- (1) Exchange between virtual assets and fiat currency.
- (2) Exchange between one or more forms of virtual assets.
- (3) Transfer of virtual assets.
- (4) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets.
- (5) Participation in and provision of financial services related to the issuance and/or sale of a virtual asset.

Article 2 of the Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises or Persons Providing Virtual Asset Services adopts the same definition for VASPs as FATF. As of the end of 2023, a total of 25 VASPs had completed AML compliance declarations, with total assets of approximately NTD5.66 billion and an operating revenue of NTD1.93 billion. Capitalization ranged from NTD500,000 to NTD126 million, indicating that the scale of VASPs is generally smaller than that of traditional financial institutions. To enhance AML supervision of VASPs in Taiwan, on November 30, 2024, Article 6 of the Money Laundering Control Act (MLCA) was amended to introduce a registration regime and criminal liability for unregistered VASPs. Pursuant to Paragraph 2 of Article 6 of the MLCA, the Financial Supervisory Commission formulated the Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises or Persons Providing Virtual Asset Services. These regulations cover business categories, segmented registration, conditions and procedures, operator administration, and transitional provisions. The new regulations took effect on November 30, 2024.

Virtual asset transactions and transfers may occur through exchanges or trading platforms using methods such as online transfers, ATM transfers, convenience store code payments, or over-the-counter (OTC) payments via peer-to-peer private agreements. OTC payment methods include bank transfers or in-person cash payment, and the sector features higher structural complexity, with a high degree of integration with other sectors such as financial institutions and convenience stores, allowing for rapid and significant movement of funds.

The flow of virtual asset trading can be categorized into crypto-to-crypto and fiat-to-crypto transactions. Crypto-to-crypto trading refers to the exchange of one virtual asset for another. As these transactions do not pass through the banking system, they fall outside the bank's monitoring scope. While all VASP operations are physically located within Taiwan, transactions occur online, permitting users to complete transactions without using third-party financial institutions and rendering business activities unrestricted by national borders.

Virtual assets possess economic value, cross-border transferability, rapid settlement, and decentralization. In addition to exchange and platform-based trading, holders can use network protocols to transfer or make payments with virtual assets. By entering a wallet address and confirming the transaction, large sums can be moved without involving any controlling institution or generating cross-border transaction records, making virtual assets particularly vulnerable to criminal misuse for ML.

The cross-border transferability of virtual assets may also be exploited by criminal groups for laundering. For example, criminal organizations may funnel fraud proceeds into front accounts they control, transfer those funds to a designated VASP wallet, and then convert the proceeds into virtual assets for deposit to an account registered with an offshore VASP—ultimately moving illicit funds overseas under real-name authentication. Assets may then be transferred to additional wallets designated by VASPs for laundering.

Domestic VASPs in Taiwan provide the following services:

- (1) Buying and selling virtual assets for customers: In 2023, the total transaction value was approximately NTD201 billion.
- (2) Crypto-to-crypto exchange for customers: In 2023, the total transaction value was approximately NTD162.7 billion.
- (3) Transfer of virtual assets for customers: In 2023, the total transfer value was approximately NTD237 billion.
- (4) Custody of customers' virtual assets: In 2023, the total value held in custody was approximately NTD14.7 billion.
- (5) Providing underwriting and related services for customer virtual asset issuances: In 2023, the total amount issued was 0.

Because virtual assets use blockchain technology, all transactions are immutably recorded on-chain, making all transaction histories publicly verifiable. However, wallet addresses consist of random alphanumeric strings that are not linked to real-world identities, which gives virtual assets a high degree of anonymity. In addition to trading on domestic and foreign trading platforms, virtual asset transactions may take place on OTC markets through private agreements, OTC peer-to-peer trades, OTC platform trades, bitcoin automated teller machine (BTM), or convenience store payment collection—resulting in highly diversified payment and service channels with high structural complexity.

In summary, owing to the high anonymity, economic value, decentralization, cross-border transferability, and rapid settlement features of virtual assets and related services, the VASP industry is increasingly used for ML, resulting in an overall risk rating of “very high”.

Case Study

Starting in 2018, Person A, the head of Group A, established nearly ten companies, including Company B in Taiwan, to operate cross-border online gambling businesses. These entities employed personnel across financial, technical, customer service, and other functions. In the name of Group A, Person A developed gambling games based in Taiwan and ran servers to provide platform rental services to overseas gambling operators, earning profits in excess of NTD126.66 million. To transfer illicit proceeds from abroad to Taiwan, Person A used company networks, underground banking, and additionally laundered funds through virtual currency wallet accounts.

In 2018, Person A planned and established an underground banking ring handling cross-currency exchange in RMB, HKD, NTD, USD, PHP, and other foreign currencies and virtual currencies. Cross-border fund delivery and receipt were conducted through domestic remittances or cash transactions as well as via foreign accounts of gambling clients or partner underground banking operators abroad. Within the ring, employee B was responsible for soliciting clients wishing to exchange PHP, RMB, HKD, USD, other currencies, or Tether (USDT), onboarding them via Telegram, WhatsApp, WeChat, Line, etc. Employee C would then confirm currency and amount with clients in messaging groups. For exchanges involving Tether, the day's conversion rate was based on the prevailing USD/NTD rate quoted by Bank of Taiwan.

Once a customer agrees to the currency exchange, if the transaction involves converting NTD or Tether into other foreign currencies, an external agent first goes to the agreed location to collect the NTD cash from the exchange customer and upstream provider in Taiwan or receives exchange funds from the exchange customer via a virtual currency wallet account or a domestic financial account; then, the agent arranges for the exchange funds to be paid into the exchange customer's designated account through an overseas financial account or virtual currency wallet account. If the exchange customer wishes to convert other foreign currencies or Tether into NTD, then a virtual currency wallet account and an overseas financial account are provided to receive the exchange funds from the customer, after which an external agent visits the agreed location to pay the NTD cash to the exchange customer in Taiwan. Subsequently, the external agent deposits, withdraws, or transfers the funds in the account to an account, virtual currency wallet, or cash storage location under the actual management of Group A. The daily transaction amount and exchange rate for each client are logged in daily reports, and underground banking ledgers and preliminary monthly profit reports are prepared monthly for A's profit settlement. Through these methods, criminal proceeds collected as commissions for platform rental services to overseas gambling operators by Group A are brought from overseas into Taiwan and converted into NTD cash or Tether. Thus, the group jointly and unlawfully engages in cross-border foreign exchange activities involving NTD, RMB, HKD, PHP, USD, etc., between Taiwan, Mainland China, Hong Kong, the Philippines, Cambodia, Thailand, the United States, and other regions, with handled exchange amounts totaling at least NTD21.7 billion, and total profits of at least NTD126.66 million, creating transaction cut-offs to disguise and conceal the nature, source, or destination of the criminal proceeds through the aforementioned methods.

Source: Investigation Bureau, Ministry of Justice

3. Very High-Risk Vulnerability: Domestic Banking Units (DBUs)

| Assessment period | 2021 | 2024 |
|-------------------|------------------|------------------|
| Rating | Very High | Very High |

As of December 31, 2023, there were a total of 38 domestic banks in Taiwan, with total assets amounting to NTD59.8 trillion, total loans of NTD35.5 trillion, and total deposits of NTD50.8 trillion, making them among the most important components of the national financial system. Domestic banks in Taiwan offer diverse services, with some banks providing wealth management for high-net-worth clients, resulting in relatively complex business structures. A high proportion of domestic banks are affiliated with large financial groups and maintain close integration with other sectors. They operate 3,393 branches across Taiwan and 641 branches internationally, reflecting their broad and far-reaching presence.

The banking business encompasses deposits, remittances, private banking, and trade finance. As deposit accounts offer cash payment and monetary instrument services, most transaction flows enter or exit through deposit accounts, and the frequent use of front accounts is observed. Additionally, remittance services enable cross-border fund transfers and can involve higher-risk activities, such as private banking and trade finance, highlighting the elevated product and service risks of domestic banks.

Domestic banks primarily serve Taiwanese clients, mostly maintaining ongoing business relationships, although some transactions are occasional. Certain intermediary services, such as correspondent banking, involve indirect clients and continue to present a degree of ML/FT risk. Furthermore, nearly all customer types engage in banking relationships with domestic banks—including politically exposed persons (PEPs), high-net-worth individuals, and legal entities with opaque beneficial ownership—resulting in an elevated risk profile.

Participation in international activities is significant, with large volumes of international remittances and trade finance conducted each year. Overseas expansion is achieved through 641 branches abroad, with the top three regional locations being Southeast Asia (50.08%), East Asia (32.76%), and the Americas (12.64%). As of the end of 2023, individual and entity clients from FATF-designated high-risk jurisdictions made up 0.88% and 0.44% of customer bases, respectively; in 2023, inward and outward transactions with these jurisdictions accounted for 0.31% and 0.37% of total yearly inward and outward transaction volumes.

Service channels are varied, and as Taiwan continues to promote non-cash transactions, in-person banking is less common; most transactions are conducted via non-face-to-face channels, including online banking and ATM services, adding a degree of anonymity. In 2023, non-face-to-face outward transactions reached 1.37 billion transactions, representing 77.41% of all outward transactions, an increase of 24.8% compared to 2020. ATM interbank transactions reached 445.23 million times, interbank withdrawals totaled 342.16 million, and cross-border withdrawals using UnionPay cards amounted to 2.96 million. Due to the high level of anonymity associated with these transactions, they present a degree of ML and FT risk to financial institutions.

In summary, domestic banks offer deposit accounts that involve cash handling and the use of monetary instruments, as well as remittance services that facilitate cross-border fund transfers, reflecting considerable fund mobility. The client base is broad, and activities involve

high-risk and watch-list jurisdictions. Service channels include non-face-to-face transactions, making the sector particularly susceptible to ML. In practice, many cases have involved the misuse of bank products and services for laundering purposes, resulting in an overall risk rating of “very high”.

Case 1

Person A registered Company A, promptly opened a bank account under the company’s name, and then handed over the passbook, ATM card, and password to a member of a fraud ring. After obtaining the physical account details, members of the fraud ring approached third-party payment companies, such as Company B and Company C, to apply for collection services. They then obtained virtual collection account numbers and subsequently defrauded Person B, who had been deceived by a fake investment opportunity, into remitting funds into the virtual account.

Source: Investigation Bureau, Ministry of Justice

Case 2

Person A, an employee of Bank A, joined a fraud ring and instructed 11 individuals, including B, a front account provider within the ring, on how to respond during in-person counter applications to successfully link Taiwan dollar and foreign currency–contracted accounts and raise the transfer limits of these accounts. During A’s work hours, they raised the online banking daily transfer limits for the front account providers to between NTD10 million and 15 million and designated the beneficiary of international remittances as B cryptocurrency platform accounts, earning fees of NTD40,000 or more per transaction.

Fraud ring C and other fraud rings successively established fraudulent investment platforms or created false investment scam rings on communication software. After fraud ring C obtained the front account information of bank A, members of the fraud ring used electronic communications or the internet to disseminate information under the pretext of investing in stocks, foreign exchange, and futures to the general public and randomly invited investors to join the platform or ring. As a result, investors followed the instructions of fraud ring members and remitted investment funds into the aforesaid front accounts before realizing they could not withdraw their profits and were thus defrauded. The illicit funds were either withdrawn in cash by couriers or transferred by members of the fraud ring through front accounts and virtual asset trading platforms. These proceeds were moved from front accounts to designated B virtual currency trading platform accounts, either via cash withdrawal or virtual asset purchases, thereby constituting ML activities.

Source: Investigation Bureau, Ministry of Justice

4. High-Risk Vulnerability: Offshore Securities Units (OSUs)

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

Since March 2014, the Financial Supervisory Commission has gradually approved OSU licenses, making this a relatively new sector. Customers permitted to purchase OSU products are limited to domestic professional investors and foreign non-resident individuals and entities, making customer acquisition challenging and constraining the business scale. In 2023,

18 securities firms operated OSU services for approximately 2,380 customers; in 2023, total OSU operating income was about NTD7.38 billion, comprising just 3.91% of the securities sector's overall revenue of NTD188.6 billion in 2023.

OSUs may provide a wide range of services, including various types of securities services (such as securities brokerage, proprietary trading, underwriting, wealth management, OTC derivatives business, and foreign exchange services) and products consisting of various types of foreign currency financial instruments (such as stocks, bonds, futures, structured products, derivatives, fund certificates, and foreign exchange products, but excluding insurance products). The origin of these products may be global, offering diverse and extensive service types and product ranges. However, as OSU operations remain relatively small in scale, the revenue is concentrated in specific business lines. According to current statistics on OSU business practices, in 2023, 97.88% of OSU operating income was derived from proprietary securities trading, with other securities businesses accounting for a smaller proportion.

OSU mainly undertakes foreign-currency-denominated products, often involving investment in offshore products. The services are limited to domestic professional investors and offshore non-residents. Trading in offshore financial products—such as equities and funds—is predominantly conducted on a continuous basis, though one-off transactions may also occur. These features present ML/FT vulnerabilities. OSU primarily plans to expand its client base by focusing on offshore non-residents. These clients may be globally dispersed and could include domestic and foreign PEPs. Implementing CDD under these conditions is challenging, indicating potential ML/FT risks. As of the end of December 2023, OSU client composition statistics show that 24.37% of clients (accounts) are professional institutional investors (i.e., financial institutions), 16.05% are professional investment entities or individuals, and 59.58% are retail investors. Overall, the client profile is dominated by overseas retail investors. However, based on transaction value statistics, considering the proprietary trading business accounts for 97.88% of OSUs' total operating income, the 2023 proprietary trading transaction value shows that professional institutional investors accounted for 90.65% of the total proprietary trade volume. Therefore, OSUs' overall business volume is mainly derived from professional institutional investors.

OSUs mainly target offshore non-residents as their customer base, offering tax benefits for products sold to this group. Clients may be located worldwide. In addition, concerning products, OSUs offer a broad product range, possibly including products issued worldwide, with business activities potentially involving high-risk jurisdictions.

OSUs permit order placement through non-face-to-face channels such as internet and telephone. Furthermore, OSUs are prohibited from accepting or disbursing foreign currency cash; all transactions are conducted through banking systems.

Considering that OSUs provide diverse and complex products, are highly integrated with other industries, and attract overseas clients through tax incentives, their clientele may be globally dispersed and include offshore non-resident, carrying inherent ML/FT risks. Therefore, OSUs are assessed as having an overall “high risk” level.

5. High-Risk Vulnerability: Branches of Foreign Banks in Taiwan

| Assessment period | 2021 | 2024 |
|-------------------|------|------|
| Rating | High | High |

As of the end of December 2023, total assets of foreign bank branches in Taiwan amounted to NTD5.08 trillion, representing only 8% of domestic banks' total asset size. Deposits accounted for merely 3% relative to domestic banks, indicating a small overall scale in Taiwan's banking industry. As of the end of December 2023, there were 28 foreign bank branches, including 3 from Mainland China, all affiliated with head offices ranked among the world's top 500. Among the 31 foreign bank branches in Taiwan, 26 operate solely through a Taipei branch, while 5 have established branches in Taichung or Kaohsiung. The number of branches represent only about 1% of domestic banks. Foreign bank branches in Taiwan primarily provide financial services to domestic professional institutional investors and large enterprises; services include cross-border remittances and trade finance. A few banks also engage in wealth management, often leveraging their international networks, enabling them to provide diverse financial services.

Services offered by foreign bank branches in Taiwan include corporate banking, trade finance (such as export letters of credit), online foreign-exchange trading, correspondent banking, and wealth management. Individual branches tend to focus on specific business areas rather than offering all products to customers. Funds are primarily deployed through interbank deposits and borrowings with foreign correspondent banks, lending, and trading in financial assets. Some branches also engage in securities agency businesses, such as the brokerage of foreign bonds (a securities business), or provide advisory services for offshore derivative financial products. Their main clients are head offices or correspondent banks (from which they receive revenue sharing). A small number manage trust-based investment fund businesses by cooperating with securities investment trust enterprises for commission-based sales. Given that most business involves cross-border financial services for corporate clients, their operational structures are relatively complex.

Most clients of foreign bank branches in Taiwan are publicly listed companies (with higher transparency), large corporations, high-net-worth individuals, and professional institutional investors, with few occasional clients. Client relationships tend to be long-term and direct. However, clients may conduct transactions through complex legal agreements, making the verification of beneficial ownership more challenging. There may also be opportunities for relationships with domestic and foreign PEP, presenting ML/FT vulnerabilities. However, PEPs do not constitute a significant portion of the client bases of foreign bank branches in Taiwan.

The proportion of clients or transactions involving high-risk jurisdictions is very low for foreign bank branches in Taiwan. As of the end of 2023, corporate clients from high-risk jurisdictions accounted for approximately 0.33% of all corporate clients, while individual clients from such jurisdictions represented around 0.2% of all individual clients. Inward remittances involving high-risk jurisdictions comprised about 0.13% and outward remittances about 0.33% in 2023. Considering that these clients remain active and transactions may continue and that foreign bank branches utilize their groups' international networks for cross-border remittances and correspondent banking, which may involve high-risk jurisdictions, there remains a certain degree of risk.

In addition to in-person services by staff, foreign bank branches in Taiwan facilitate non-face-to-face transactions through internet, mobile, telephone, or fax instructions. In 2023, non-face-to-face outward transactions conducted by foreign bank branches accounted for approximately 82.12% of all outward transactions (including face-to-face and non-face-to-face).

Overall, foreign bank branches in Taiwan, as part of foreign head offices or groups, are capable of facilitating rapid fund transfers and a broad range of financial services through their group networks. Their clientele primarily consists of professional institutional investors and large corporations. Given that clients may transact under complex legal agreements and beneficial ownership verification is challenging, the overall risk rating is “high”.

6. High-Risk Vulnerability: Offshore Insurance Units (OIUs)

| Assessment period | 2021 | 2024 |
|-------------------|------|------|
| Rating | High | High |

OIUs have been granted licenses and commenced operations progressively since June 2015, representing a relatively short operating history compared with other sectors. Because the insured and policyholders for OIU insurance products must be foreign nationals, the client base is limited, resulting in a smaller operational scale. In 2023, OIU life insurance premium income amounted to approximately NTD750 million, accounting for a minimal share (about 0.03%) of the total life insurance premium income (around NTD2.2 trillion). Currently, 20 insurers have been licensed, including 15 life insurers, 4 property insurers, and 1 reinsurer.

OIUs predominantly offer personal insurance products, including interest-sensitive whole life insurance, variable life insurance, and variable universal life insurance, which are high savings or investment-linked insurance products. Such products may be linked to various investment targets and differ significantly from standard protection-type insurance products. Additionally, for OIU clients, insurance payouts and income derived from investment targets linked to investment-type policies may be exempt from withholding income tax. This tax advantage could attract offshore clients with diverse insurance purposes.

The clientele for OIUs must be foreign individuals or foreign legal persons. As of the end of 2023, foreign individuals accounted for 2.15% and foreign legal persons accounted for 97.85%. Among the clients, foreign PEPs represented 1.77% and high-net-worth individuals 0.25%. OIU transactions involve cross-border products or services, making it more difficult compared with domestic insurance businesses to verify clients’ true occupations or beneficial ownership.

As of 2023, the main sales targets of OIU were individuals from Mainland China, Japan, South Korea, and Thailand. Clients from or registered in tax havens accounted for approximately 1.01%. There were no insured parties from North Korea or Iran; however, clients may still come from other high-risk jurisdictions.

OIU life insurance business primarily involves policies taken out in person by clients, while property and casualty insurance, as well as reinsurance business, is conducted mainly with foreign legal entities. As of the end of 2023, the proportion of face-to-face transactions reached 59.17%, with this segment consisting chiefly of reinsurance business conducted between insurance companies and reinsurance companies. OIU policy agreements may be signed by agents; distribution channels include not only the insurer’s own agents but also third-party insurance brokers or insurance agents. By the end of 2023, 62.09% of services had been provided through insurance brokers, insurance agents, or bank distribution channels.

Because OIU business is primarily conducted in foreign currencies, targets offshore clients, and primarily involves insurance and reinsurance contracts, identifying the ultimate actual beneficiary is inherently challenging. Currently, most insurance policies issued

are high-savings products, which carry a higher risk of ML. Additionally, a significant proportion of OIU services is distributed through non-insurer channels, resulting in an overall risk rating of “high”.

7. High-Risk Vulnerability: Securities Firms

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

As of the end of 2023, there were 65 dedicated securities firms. These firms operated a total of 746 branch offices in Taiwan and 70 subsidiaries in other regions, including 38 in Hong Kong, 9 in the British Virgin Islands, 6 in Mainland China, and 5 in the Cayman Islands. By the end of 2023, the total assets of all securities firms amounted to NTD2.55 trillion, representing about 2.05% of the financial sector’s total assets. Securities firms’ business income primarily comes from brokerage commissions. In 2023, the total trading volume in the securities market was NTD67.21 trillion, with brokerage business income at NTD97.91 billion and profits of approximately NTD58.15 billion.

The main business lines for securities firms are brokerage, proprietary trading, and underwriting of securities. Wealth management services are also offered but at a limited scale. Securities firms neither provide payment products or services involving cash or monetary instruments nor offer trade finance or cash transfer services. The fund flows arising from clients’ purchases and sales of securities products are primarily processed through banks, and the business nature is straightforward. However, securities products have the characteristics of high value and high liquidity, facilitating rapid fund transfers and obscuring the origins of funds.

Securities firms’ clients are mainly domestic, with a small share of foreign individuals and both foreign and domestic PEPs, presenting certain ML and FT vulnerabilities. As of the end of 2023, there were 12,512,163 cumulative securities accounts, including 12,418,637 for natural persons and 93,526 for corporations. Between 2021 and 2023, investments by foreign natural persons and foreign legal persons accounted for approximately 14.24% of total investment amounts.

Foreign corporate clients of securities firms may originate from high-risk jurisdictions such as the United States, Singapore, and the British Overseas Territories. While their transaction volumes constitute a small proportion of total business (as of 2023: 2.73% from the United States, 0.53% from the British Territories, and 1.61% from Singapore), these transactions occur regularly and continuously. Securities firm operations may involve tax havens and other jurisdictions of concern. Even when entrusted with overseas securities transactions, the types of securities and exchanges must be approved by the Financial Supervisory Commission. In 2023, transaction volume by Taiwanese traders in the United States and Hong Kong—two regions with high Financial Secrecy Index (FSI) rankings—accounted for 85.21% of all overseas securities transactions.

Most brokerage transactions at securities firms are conducted through online platforms and voice channels. Anonymity risks arise where orders are placed through third parties or executed via front accounts. Brokerage trading volumes make up a significant portion of total operations. As of the end of 2023, electronic trading accounted for approximately 77.73% of securities market turnover.

Securities firms provide securities trading-related services and are highly integrated with other financial institutions. Additionally, the cash flow from securities brokerage business primarily goes through banks, and the cash flow of securities trading is returned to accounts under the same name. Clients of securities firms cannot use securities products to transfer funds; however, anonymity concerns arise when clients entrust third parties to place orders or use nominee accounts for trading. Underwriting business clients have also provided nominee accounts to participate in allocations, potentially involving securities crimes (e.g., insider trading, market manipulation, and securities fraud). Therefore, the overall risk rating is “high”.

8. High-Risk Vulnerability: Jewelry Businesses

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

According to the business scope and definitions provided by the Ministry of Economic Affairs, the jewelry businesses encompass the manufacturing, wholesale, and retail of jewelry, precious metals, and ornaments, including related import and export activities. The jewelry industry is not a licensed business sector, resulting in a large number of operators totaling 4,672 entities (including companies and firms), of which 58% are firms and 42% are companies. In terms of capital, the average capital per entity is approximately NTD3.45 million (about USD105,000), mostly small-scale firms primarily engaged in the wholesale and retail of gold (and silver) ornaments and jewelry. Please refer to the table below for a statistical overview of the number of jewelry industry entities and their average capital.

Jewelry Industry Overview: Number of Companies and Firms and Average Capital Statistics

As of the end of 2023

| Capital Range (NTD) | Number of Entities | | Average Capital (NTD) | | Average Capital (NTD) |
|----------------------------|--------------------|-------------|-----------------------|------------|-----------------------|
| | Company | Firm | Company | Firm | |
| 30,000,001 and above | 63 | 1 | 134,177,737 | 65,000,000 | 133,096,835 |
| 20,000,001 to 30,000,000 | 44 | 0 | 26,311,364 | 0 | 26,311,364 |
| 10,000,001 to 20,000,000 | 82 | 0 | 15,173,364 | 0 | 15,173,364 |
| 5,000,001 to 10,000,000 | 175 | 6 | 8,065,842 | 5,616,667 | 7,984,654 |
| 1,000,001 to 5,000,000 | 638 | 62 | 3,576,212 | 2,154,645 | 3,450,302 |
| 500,001 to 1,000,000 | 548 | 120 | 978,359 | 896,775 | 963,703 |
| 0 to 500,000 | 416 | 2,517 | 344,360 | 229,553 | 245,836 |
| Subtotal / Overall Average | 1,966 (42%) | 2,706 (58%) | 7,745,500 | 339,130 | 3,455,766 |
| Total Entities | 4,672 | | | | |

Source: Department of Commerce, Ministry of Economic Affairs

According to the Ministry of Finance’s fiscal statistics database, the annual wholesale and retail sales of the jewelry industry were approximately NTD50.1 billion in 2021, about NTD69.1 billion in 2022, and about NTD78.6 billion in 2023. Among them, the six major municipalities accounted for more than 90% of total sales (about 91% in 2021, about 94% in

2022, and about 93% in 2023). The jewelry industry's annual sales accounted for approximately 0.23% of GDP in 2021, about 0.3% in 2022, and roughly 0.33% in 2023. Overall, due to the impact of the COVID-19 pandemic (hereinafter referred to as COVID-19), the jewelry industry was at its weakest in 2021. In 2022, as the pandemic subsided, along with government stimulus measures and economic recovery, the overall business condition of the industry had significantly improved by the end of 2023 compared to 2021.

Jewelry businesses sell products such as gold bars, platinum bars, loose diamonds, gold jewelry, platinum jewelry, and other types of precious metals and jewelry. These items generally have high unit prices and value, are small in size, easy to transport and liquidate, and have a global market. Payment methods include cash, credit cards, bank transfers or remittances, checks, and gift certificates. Monitoring abnormal transaction prices is more challenging in the precious metals and jewelry market, especially for diamonds, which are typically priced individually. Gold and platinum bars, as well as loose diamonds, offer high liquidity and a broad market, and a very high likelihood of resale. In contrast, gold jewelry and other pieces are less easily moved and tend to incur higher losses when transferred. In investigations of illegal fundraising and fraud cases, it is often found that criminals use illicit proceeds to purchase gold or high-value jewelry.

Jewelry businesses have a broad customer base with no identity restrictions, and precious metals and jewelry are not controlled items, lacking an ownership registration mechanism; this makes it difficult to ascertain the true identities and transaction purposes of customers. According to local customs, most jewelry customers are repeat clients who typically purchase gold and silver jewelry or bars as gifts for festivals and special occasions. However, jewelry businesses often have limited knowledge of their customers beyond their regulars.

Taiwan lacks raw material resources for precious metals and jewelry, so gold and jewelry businesses are heavily reliant on imports. According to the Ministry of Finance import and export trade statistics, the top seven import regions before 2023 were Japan, Hong Kong, Switzerland, Mainland China, the United States, South Korea, and Singapore. While these countries are not designated as high-risk jurisdictions by the FATF, they ranked high in the 2022 Financial Secrecy Index (FSI), indicating that the associated risk remains very high.

Most gold and jewelry transactions are conducted face-to-face; however, owing to the impact of COVID-19 and advancements in digital and cloud technology, more businesses are using e-commerce platforms for sales. These sales primarily involve low-value products that do not serve as ML tools.

In summary, as gold and jewelry have high liquidity, customer identities and transaction purposes are often difficult to verify, and the industry has significant exposure to high-risk countries, the overall risk rating is "high".

9. High-Risk Vulnerability: Postal Institutions Handling Savings and Remittances

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

In Taiwan, the only institution engaged in postal savings and remittance business is Chunghwa Post Co., Ltd. (hereinafter referred to as Chunghwa Post). As of the end of December 2023, Chunghwa Post had total assets of NTD8.33 trillion, and total deposits of NTD7.15 trillion. As of the end of December 2023, Chunghwa Post had one head office and 1,296 branches. Branches are classified into five tiers based on their deposit balances. These branches are spread across cities, rural areas, outlying islands, and remote regions, offering convenient and accessible financial services that may be relatively vulnerable to misuse as channels for ML.

Chunghwa Post Co., Ltd. provides various financial products and services, including deposit services through its postal savings department, international remittances, postal gift certificates, and online banking. Its life insurance department offers simplified life insurance, policy loans, and real estate mortgage loans, while the postal department manages cash bags and other related services. The overall operational activities primarily derive from the savings and remittance business.

As of the end of December 2023, the number of depositors using Chunghwa Post's savings and remittance services exceeded 24.37 million, with depositors spread throughout the country and having frequent interactions with the company. Chunghwa Post's financial service clients are mainly individual account holders, with transactions being relatively straightforward in nature, and the company maintains continuous and direct relationships deeply rooted in local communities. The proportion of foreign clients establishing business relationships with Chunghwa Post is very low, representing a minor share of overall operations. Chunghwa Post's financial service clients are predominantly local natural persons with relatively simple occupational profiles. The proportion of foreign clients is very low, primarily consisting of employed foreign laborers using the service for salary transfers. Domestic PEPs may include local councilors, bureau chiefs of local government, and township representatives, but their proportion is low. The proportion of high-net-worth clients is also relatively low compared with that in the banking industry.

Chunghwa Post's savings and remittance services related to cross-border transactions are limited to international remittances, with a relatively small number of transactions. Chunghwa Post commenced its foreign exchange remittance services in September 2022, transitioning to in-house processing of Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages, replacing the previous outsourced arrangement. While these activities do not constitute a significant portion of the company's overall operations, some cross-border transactions may still involve high-risk jurisdictions.

With technological advancements, Chunghwa Post's customer service model for savings now includes, in addition to face-to-face and agent (counter) transactions, options such as online banking, mobile post office services, telephone banking, and ATMs. Since March 2022, Chunghwa Post has offered digital deposit accounts, allowing adult domestic customers to open accounts online or via mobile devices without visiting physical branches. The growing use of these non-face-to-face channels raises concerns about increased transaction anonymity.

In summary, Chunghwa Post operates in widespread locations, making it relatively susceptible to misuse as a channel for ML. In September 2022, the company began processing foreign exchange remittances in-house through SWIFT messages, replacing the previous outsourcing arrangement. Some cross-border transactions may involve high-risk jurisdictions, and the rise in non-face-to-face transactions raises concerns about anonymity. In recent years, cases have been reported where fraud groups have exploited accounts provided by Chunghwa Post as front accounts for ML. Therefore, the overall risk rating is "high".

Case 1

Mr. A and his son, former employees of labor brokerage firms, including Company A, have been engaged in the foreign labor brokerage business for many years. To receive, hold, or use illicit proceeds, such as mediation fees from foreigners illegally employed as caregivers and illegal wages paid by employers, Mr. A accompanied Company A in 2018 and 2021 in recruiting both legal Indonesian caregiver B and unregistered migrant worker C to apply for Chunghwa Post savings accounts. He then purchased their account passbooks, ATM cards, seals, and passwords for NTD5,000 each. Subsequently, Mr. A instructed some employers to transfer caregiving fees into the accounts of these individuals. Mr. A would withdraw the illicit proceeds from these accounts every 5–6 days at different post offices, creating a disruption in the money flow to conceal or disguise the source of the illicit proceeds. Since unlawfully obtaining the accounts of these individuals, the accumulated illicit proceeds have amounted to over NTD25.32 million.

Source: National Immigration Agency, Ministry of Interior

Case 2

Mr. A, a public servant, knowingly assisted his girlfriend, Ms. B, in concealing illicit proceeds from organized fraud. He deposited the illicit cash provided by Ms. B into his own financial accounts at domestic banks and postal institutions; thereafter, he purchased real estate and paid for renovation in his own name, thus creating money flow disruptions, with a total amount of over NTD14.22 million involved.

Source: Agency Against Corruption, Ministry of Justice

10. High-Risk Vulnerability: Life Insurance Companies

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

As of the end of December 2023, there were 21 life insurance companies operating in Taiwan, comprising 19 domestic life insurance companies and two branches of foreign life insurance companies. The total assets of the life insurance industry amounted to NTD34.9 trillion, with premium income of approximately NTD2.19 trillion.

Currently, life insurance companies in Taiwan may either establish or join financial holding companies to leverage cross-sector synergies within financial conglomerates. Those not affiliated with financial holding companies can expand their operations through strategic alliances with banks or securities firms or by distributing insurance products via insurance agents and brokers. In 2023, the life insurance industry's first-year premium income was primarily derived from bancassurance channels (including bank agencies and brokerages), which accounted for 41.75%, while traditional agency and brokerage channels contributed 18.27%. The share of first-year premium income from bancassurance exceeded that from the companies' own marketing systems, reflecting a considerable level of integration between the life insurance industry and other financial sectors.

The insurance products offered by life insurance companies include life insurance, health insurance, accident insurance, and annuity insurance. In 2023, total premium income for the life insurance industry was NTD2.19 trillion, of which life insurance accounted for NTD1.49 trillion (68.1% of total premiums), health insurance NTD433.6 billion (19.8%), annuity insurance NTD190.7 billion (8.7%), and accident insurance NTD73.2 billion (3.3%). Among insurance products, those most susceptible to misuse for ML purposes are those with policy value reserves or cash value, such as life insurance, investment-linked insurance, and annuity insurance—products that represent a significant proportion of overall premium income in the market. Additionally, perpetrators of insurance-related ML often pay premiums in a lump sum when purchasing life or annuity insurance and then surrender the policy during the free-look period (or a short period thereafter) or later obtain policy loans, with the goal of laundering illicit proceeds.

In principle, both domestic and foreign individuals are eligible to purchase life insurance products, which may include high-net-worth individuals or PEPs. Furthermore, insurance premiums may be paid not only by the policyholder but also by the insured or beneficiary. Given the diversity of the life insurance industry’s customer base and payment sources, there is a certain degree of ML risk.

The operational scope of the life insurance industry is primarily domestic, with relatively few overseas branches, mostly located in Mainland China, Hong Kong, Vietnam, and South Korea. Notably, Vietnam was classified as a high-risk jurisdiction on June 23, 2023. Although the current share of premium income from overseas branches is not high, their business activities may be distributed across high-risk jurisdictions.

The life insurance business is sourced through both direct marketing (insurance companies selling directly to consumers) and indirect marketing (sales via other financial institutions, including insurance brokers and agents, through joint marketing or strategic alliances). Sales methods in the life insurance industry can be categorized into two types: face-to-face sales, conducted by company representatives through in-person interactions, and non-face-to-face sales, which are carried out via online platforms or telephone channels. Due to the diversity of distribution channels and the high proportion of indirect marketing, there is a certain degree of ML risk.

In summary, as many life insurance products have policy value reserves or cash value and can be sold through various channels—such as insurance sales agents and insurance brokers and agents, as well as through online and telephone marketing—criminals may, in practice, pay lump-sum premiums and then terminate the contract, resulting in an overall risk rating of “high.”

11. High-Risk Vulnerability: Certified Public Accountants (CPAs)

| Assessment period | 2021 | 2024 |
|-------------------|------|------|
| Rating | High | High |

According to statistics at the end of 2023, Taiwan had approximately 4,004 practicing CPAs and a total of 2,284 CPA firms, with 60% of these firms concentrated in Taipei City, New Taipei City, and Taoyuan City. Accounting services that may be subject to the MLCA include “tax planning”, “management consulting”, and “business registration”, with a combined business income of NTD4.6 billion, accounting for 12.65% of total business income (NTD36.56 billion). The transaction volume statistics are as follows: As of the end of 2023,

there were a total of 61,917 service cases handled by CPA firms, comprising the following: 6,961 cases (11%) for tax planning, 9,177 cases (15%) for management consulting, and 45,779 cases (74%) for business registration. Although there is a lack of specific statistical data, the transaction amounts handled by CPAs when conducting transactions listed under the MLCA may be relatively high. Taking merger and acquisition (M&A) services provided by CPAs as an example, according to the 2023 Taiwan M&A White Paper, there were 117 M&A transactions in Taiwan in 2022, with a total transaction amount of approximately NTD450 billion.

The accounting sector serves clients from numerous industries and business types. In the provision or preparation of relevant transactions on behalf of clients, CPAs also collaborate with other professionals, including those in the banking, securities, real estate, and legal sectors. In such collaborations, CPAs typically provide advisory services or issue attestation reports as required by regulatory authorities.

The services provided by CPAs in Taiwan—such as tax planning, M&As, and assisting clients in establishing overseas companies—often involve multi-layered structures; the nature and scope of these services are likely to be complex, increasing the potential for the concealment of a perpetrator's identity. CPAs possess professional knowledge of fund management and commercial transactions, and their services—including company formation, company operation or management, M&As, and financial and tax advisory—may be misused for illicit purposes.

Regarding client relationships, the clientele of CPAs spans various professions and sectors and may include high-net-worth individuals; however, related data and proportions are currently unavailable. CPAs may accept cross-border engagements to conduct transactions stipulated in the MLCA, including those involving clients or transactions that could be associated with high-risk jurisdictions. According to the 2022 CPA Firm Service Industry Survey Report, 19 firms conducted business operations in Mainland China. Among their services, those involving AML-related business (such as investment assessment and consulting) accounted for approximately 14.7%, with professional income totaling around NTD46.06 million. For cross-border M&A cases, such services are typically provided by local CPA firms in the respective country. However, in cases where foreign companies acquire Taiwanese enterprises, CPAs in Taiwan could be involved.

As for service channels, professional ethics impose strict restrictions on accountants' advertising, accountants rarely make contact with clients through referral channels. Non-face-to-face service channels are rarely used, except in limited cases where CPAs assist foreign investors in opening custodial accounts with banks or securities firms. Some business registration services may come through referrals from certified public bookkeepers or bookkeeping and tax return filing agents.

In summary, transactions conducted by accountants within the scope of the Anti-Money Laundering Act often involve high-value amounts. CPAs possess professional knowledge of fund management and commercial transactions, and their services—including company formation, company operation or management, M&As, and financial and tax advisory—may be misused for illicit purposes. CPAs are highly familiar with financial and tax regulations and can develop sophisticated business arrangements tailored for clients; cross-border cases may involve high-risk jurisdictions. Therefore, the overall risk rating is “high”.

12. High-Risk Vulnerability: Attorneys

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

As of December 29, 2023, there were approximately 11,998 practicing attorneys in Taiwan, with most operating as sole practitioners, partnerships, or co-locations and a small number employed by other attorneys or corporations. The number of attorneys has shown a slight upward trend compared to 2021, and as of the end of 2022, there were 4,078 law firms. According to statistics from the Directorate-General of Budget, Accounting and Statistics, Executive Yuan, the annual gross output of legal services was NTD40.57 billion in 2021, representing an slight increase compared with the total output of legal services in 2016. Attorney practices are primarily centered on litigation cases, with a minority involving non-litigation matters. In most instances, attorneys do not directly handle property but instead act as consultants providing client advisory services; however, there remains the possibility of handling large-value transactions during engagements. The business activities handled by attorneys are broad in scope. When assisting clients in preparing or executing relevant transactions—such as changes in asset ownership—attorneys typically need to work in cooperation with other industries to facilitate these transfers, resulting in a high degree of integration with other sectors.

Most attorneys engage in civil, criminal, and administrative litigation, with only a few attorneys or large law firms offering asset management consulting or cross-border legal services. Among these, domestic asset management consulting constitutes the majority, while services involving foreign assets, cross-border transactions, complex international tax planning, and multi-layered offshore company structures are relatively limited. Nevertheless, attorney services may include real estate transactions; management of client funds, securities, or other assets; oversight of bank, savings, or securities accounts; financial planning for company formation, operations, or management; establishment, operation, or management of legal persons or legal arrangements; and the purchase and sale of business entities. These characteristics make the profession particularly susceptible to misuse for ML, potentially through the creation of complex company structures, operational arrangements, falsified financial attestations, trusts, or intermediaries to help criminals conceal or transfer illicit proceeds.

Attorney clients encompass a wide range of professions and industries, including natural and legal persons, domestic and foreign PEPs, high-net-worth individuals, cash-intensive businesses, and large multinational enterprises. These client segments may exploit legal professionals to achieve their ML objectives.

The scope of attorneys' business activities is predominantly domestic. Only large law firms typically possess the capabilities to provide cross-border legal services, and such services usually do not involve high-risk jurisdictions, although there remains a possibility of engaging with countries of concern.

To understand the cases and provide effective legal advice, attorneys, owing to the trust-based relationships established with their clients, generally need to interact face-to-face to verify their clients' identities and confirm facts and documentation. Only a few cases are handled via telephone, online, or through agents. Furthermore, to mitigate legal risks, attorneys typically do not accept anonymous clients. Additionally, due to strict legal requirements surrounding conflicts of interest, attorneys place a significant emphasis on verifying client identities.

In summary, attorneys engage in a wide range of business activities and serve a diverse client base. In practice, there have also been cases where criminals colluded with attorneys acting as their criminal defense counsel or legal advisors to further illicit objectives. Therefore, the overall risk rating is “high”.

13. High-Risk Vulnerability: Enterprises or Persons Providing Third-Party Payment Services (Third-Party Payment Service Providers)

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

Third-party payment service providers are entities offering integrated online payment solutions, acting as intermediaries between payers (buyers) and payees (sellers) in online transactions. These services are delivered through internet-based platforms to enhance the security, fairness, and reliability of transactions for both parties. Upon completion of an actual online transaction, third-party payment service providers receive the transaction funds and, in accordance with the consumer’s instructions, transfer the funds to the payee, serving a supervisory role to ensure performance guarantees and safeguard payment funds. This sector primarily provides escrow and payment agent services for online transactions. The total balance of escrowed and agent funds must not exceed a set limit (an average daily balance of NTD2 billion per year). Payment methods include credit cards, bank transfers (virtual accounts, online ATM), and convenience store collection (store codes, store barcodes), among others. As of December 31, 2023, there were 40 providers that had passed the third-party payment service provider registration review by the Administration for Digital Industries, Ministry of Digital Affairs.

Business models for third-party payment service providers are highly integrated with other industries. The main partners are e-commerce businesses, banks, and convenience store operators. With respect to e-commerce, the primary clients of third-party payment service providers are primarily e-commerce businesses, which can be further divided into two categories: individuals (customer-to-customer, C2C) and legal persons (business-to-customer, B2C). Regarding banking partners, third-party payment service providers establish dedicated trust accounts or performance guarantee accounts with banks to ensure the security of payments and channel credit card and bank transfer payment flows through these banks. For convenience stores, the focus is on providing collection services that enable customers to complete payments in-store for purchases made through online transactions.

Clients of third-party payment service providers are categorized into two groups: buyers and sellers. Buyer clients refer to online transaction purchasers (i.e., the general public), without specific customer identity or occupational distribution, and are mostly one-time business relationships. Seller clients are online merchants (entities selling various goods online), and these tend to be ongoing business relationships. Currently, these services are mostly limited to Taiwanese nationals or foreigners holding resident certificate, so the operational scope remains primarily domestic.

Regardless of whether the activity involves account registration or payment, interactions between third-party payment service providers and their customers occur in a non-face-to-face manner. This creates inherent anonymity risks in confirming the true identity of users and challenges in verifying the authenticity of online transactions, thereby enabling criminals to

disguise illicit funds as online sales proceeds for the purpose of ML. Although third-party payment services are not remittance services per se, when combined with bank cooperation, these services can facilitate fund transfers. The “virtual account” collection model is particularly highly susceptible to abuse by moving illegal funds due to its speed and convenience, making it difficult for law enforcement to trace money flows. Numerous law enforcement cases have shown that fraud, online gambling, and other financial crimes frequently use third-party payment platforms for ML. The sector’s relatively low entry barriers, compared with traditional financial institutions, further enable perpetrators to establish shell or single-person companies as vehicles for laundering illicit funds.

Owing to the anonymity risks inherent in third-party payment services, rapid fund transfer capabilities, increased difficulty in tracing transactions when combined with bank virtual accounts, and ongoing identification of related cases by law enforcement in recent years, the overall risk rating is “high.”

Case Study

Between August 2019 and January 2020, Person A and 13 others, intending to facilitate fraud, participated in the A-Platform fraud ring organized by defendant B and others. They provided their financial account information for use as receiving and payment accounts for victims’ investment funds. Acting as “money mules” for the group, they used virtual asset wallets opened with various VASPs to purchase Tether and other cryptocurrencies or to buy cryptocurrency in cash, make transfers, and engage in third-party payment transactions (for example, moving funds using third-party payment mechanisms in coordination with collection centers, consolidating claims from different clients, and settling illicit proceeds received by the fraud ring with other unsuspecting payees to achieve ML objectives). This method allowed them to move illicit funds into accounts designated by defendant B and others. The A-Platform fraud ring fabricated false investment return data on its website, contacting users via instant messaging applications such as LINE and other social media platforms. They claimed that the virtual currency issued by the platform would guarantee stable profits, initially attracting investors with small investments and prompt payouts to gain trust and then persuading them to invest larger sums. Through the above methods, the 14 individuals assisted in concealing or disguising the source and destination of criminal proceeds for the A-Platform fraud syndicate, with the total amount involved exceeding NTD111.29 million. Subsequently, as of January 6, 2020, A-Platform ceased website operations, leaving investors unable to request withdrawals and causing them to suffer significant losses.

Source: Investigation Bureau, Ministry of Justice

14. High-Risk Vulnerability: Real Estate Brokerage Industry

| Assessment period | 2021 | 2024 |
|-------------------|------|------|
| Rating | High | High |

Taiwan’s real estate brokerage industry includes both real estate brokerage and real estate agency. As of the end of December 2023, there were a total of 8,718 active real estate brokerage firms, including both companies and sole proprietorships. Industry estimates indicate that brokerage firms handle about 65% of real estate transactions. Based on data from the Ministry of Finance on the number of profit-seeking enterprises and sales statistics (service fee revenue

from tax filings), the total sales of the real estate brokerage industry in 2023 amounted to approximately NTD97.44 billion, with brokerages accounting for about 85% and the industry itself holding relatively few assets. The main function of the real estate brokerage industry is to accept mandates from developers or registered owners (or right holders) to handle real estate purchase and sale transactions. Upon agreement between the buyer and seller, the subsequent transfer of title is processed by a land administration agent employed by the buyer or seller, and there is generally no collaboration with other professionals such as lawyers or accountants. A small portion of firms engaged in overseas real estate also cooperate with foreign developers or brokerage companies to market or broker overseas properties for Taiwanese residents. Business locations are widely distributed across cities throughout Taiwan, including branch offices of foreign real estate enterprises.

Real estate is high in value and tends to preserve and appreciate in worth, making it susceptible to misuse as a channel for ML. Common methods include using nominee individuals or entities to acquire properties, purchasing multiple properties simultaneously, using illicit proceeds as down payments for mortgages, or buying real estate with large amounts of cash before seeking bank loans. Although the transaction value for real estate is large, payments for most transactions are processed through third-party performance escrow trust accounts. Only a small proportion of firms engage in overseas property transaction business (about 5.92% of brokerage firms have registered for overseas real estate activities, although actual involvement is estimated at less than 1%). Through brokering property purchases abroad for Taiwanese clients, funds may be transferred overseas, increasing the risk of the sector being used as a channel for ML.

Once a real estate brokerage accepts a seller's mandate for selling a property, their relationship ends upon transaction completion. With buyers, it is a one-off relationship that also ends after the deal. Clients may be natural persons, legal entities, or trust relationships and could include high-net-worth individuals, PEPs, or foreigners (including individuals from Mainland China). However, the proportion of contacts with individuals from Mainland China or other foreign countries is very low, estimated at only about 0.0049% and 0.41%, respectively.

Most real estate brokerages operate domestically, with no operations in high-risk jurisdictions. Firms that do engage in overseas real estate sales focus primarily on developed countries (e.g., the United States, United Kingdom, Japan) or emerging Southeast Asian nations (e.g., Malaysia, Thailand, Indonesia, Vietnam, and the Philippines), among which Vietnam and the Philippines are currently classified as high-risk jurisdictions.

In terms of service channels, brokerage agents and sales staff typically interact directly with both buyers and sellers. However, when buyers and sellers are represented by different brokerages, negotiation is handled by the respective agents. Additionally, it is also permissible for parties to transact through representatives. Sales of domestic real estate by overseas Taiwanese and foreigners are rare, accounting for less than 0.41%.

Given the widespread presence of brokerage outlets, the value-preserving and appreciating nature of real estate products, the allowance of transactions through agents, and the inclusion of overseas property sales among their business activities, the industry is particularly susceptible to being used as an ML conduit. Therefore, the overall risk rating is "high."

15. High-Risk Vulnerability: Agricultural Financial Institutions (including the Agricultural Bank of Taiwan and the Credit Departments of Farmers' and Fishermen's Association)

| Assessment period | 2021 | 2024 |
|-------------------|-------------|-------------|
| Rating | High | High |

As of the end of 2023, agricultural financial institutions—including the Agricultural Bank of Taiwan and the credit departments of farmers' and fishermen's association—had total assets amounting to NTD3.60 trillion, total deposits of NTD3.07 trillion, and total loans of NTD1.82 trillion. They operated a total of 1,160 branches and outlets nationwide, with no overseas branches. The credit departments of farmers' and fishermen's association are regional grassroots financial institutions with relatively simple business operations, not engaged in other financial activities, and their operations are restricted to their respective organizational regions. The Agricultural Bank of Taiwan serves as the upper-level institution for the credit departments of farmers' and fishermen's association. It is responsible for fulfilling legally mandated duties such as accepting deposits placed by these credit departments and providing operational guidance. Its business operations are largely similar to those of commercial banks.

The Agricultural Bank of Taiwan is Taiwan's only government-authorized agricultural specialized bank. Its core operations include providing financing for the agriculture, forestry, fisheries, and livestock industries in support of national agricultural policies; accepting deposits placed by the credit departments of farmers' and fishermen's association; and offering both domestic and cross-border remittance services. The credit departments of farmers' and fishermen's association primarily provide deposit, loan, payment collection, as well as domestic remittance services, which are simpler than those of commercial banks. Although the number of customers and business volume related to these services account for a relatively small proportion of the overall banking industry, the inherent characteristics of their products make them susceptible to exploitation by ML criminals; thus, they still pose a certain level of risk in practice.

The Agricultural Bank of Taiwan primarily serves farmers, fishers, agricultural and fishery enterprises, as well as the credit departments of farmers' and fishermen's association. A total of 89.59% of its deposits are interbank deposits placed by these credit departments, which operate as grassroots financial institutions with limited geographic scope restricted by regulation. Their clientele primarily consists of local farmers, fishers, and residents, making the customer composition relatively straightforward. However, some clients may include local political representatives or heads of local authorities who hold political influence (including domestic PEPs). In addition, association members are highly localized and may be subject to the influence of local political factions, serving as channels for illicit fund flows.

The scope of agricultural financial institutions' business activities is limited to domestic operations with no overseas branches. Their transactions and services mainly involve domestic economic activities. Cross-border transactions conducted by the Agricultural Bank of Taiwan are primarily limited to international remittances and trade finance, with counterparties mainly located in the United Kingdom, Hong Kong, Singapore, the United States, Luxembourg, and similar jurisdictions. The proportion of customers or transactions involving high-risk jurisdictions is very low.

Customer services at agricultural financial institutions are primarily conducted face-to-face, over-the-counter channels, although anonymous service channels such as online banking, telephone voice services, and ATMs also exist. Nevertheless, as most clients are local farmers and regional residents who use electronic devices less frequently than urban populations—and given the limited functionality and lower transaction limits of online banking, telephone services, and ATMs—anonymous non-face-to-face transactions are not the primary service channels.

In summary, due to the sizable total assets of agricultural financial institutions, the extensive nationwide network formed by the Agricultural Bank of Taiwan and the credit departments of farmers' and fishermen's association provides convenient channels for fund transfers. Customers are mostly local farmers, fishermen, and residents, some of whom may have political influence as local representatives or government heads. Association members may be affected by local political factions, serving as conduits for illicit fund flows. Coupled with the fact that the product characteristics themselves can be easily exploited by ML criminals, the overall risk rating is "high".

Cases:

A township mayor exploited opportunities related to public bidding, land leasing, and personnel appointments at the township office to solicit cash bribes from relevant contractors and personnel. To conceal illicit proceeds from bribes received over the years and evade investigation and prosecution, the mayor used a Farmers' Association account under the name of a first-degree relative, holding and managing the passbook and seal of that Farmers' Association account. The mayor deposited illicit proceeds into this account and instructed employees of the government agency where he worked to conduct irregular cash transactions, which were used to transfer or alter the illicit proceeds. Furthermore, the mayor borrowed the name of the same first-degree relative to jointly purchase land with friends using illicit bribe money, employing ML methods to conceal, transfer, and alter bribe proceeds obtained by exploiting the official position.

Source: Agency Against Corruption, Ministry of Justice

16. Medium-Risk Vulnerability: Online Gaming Business

| Assessment period | 2021 | 2024 |
|-------------------|-------------|---------------|
| Rating | High | Medium |

Online games refer to interactive entertainment conducted via the internet, including client-based Massively Multiplayer Online Games (MMOG) as well as web-based instant-play games and social media games. The online gaming industry can be broadly divided into three types: game developers, game operators, and game point vendors. Most game developers engage in business-to-business (B2B) relationships—with revenues primarily derived from licensing fees, development outsourcing fees, and other sources—and do not directly handle payment transactions with consumers. Game operators focus on game operation, agency operation, and provision of gaming platforms or services, generating revenue mainly from game sales, platform subscriptions, advertising, and similar sources. Game point vendors are businesses that issue game points, with their primary revenue coming from sales of points within game stores. Among the various business types in the online gaming industry, game

point cards sold by game point vendors have a stored-value function. These cards are bearer instruments that do not require user identification, and their serial numbers, being intangible, are easily transferable prior to value loading. Their high liquidity makes them susceptible to misuse by criminals for transferring illicit funds.

Currently, there are five major game point vendors in Taiwan, with two vendors dominating most sales channels and cross-industry cooperation. Sales channels are primarily divided into physical point card sales and online game point sales. Physical sales commonly occur in convenience stores, large retail stores, and similar outlets, while online sales are primarily conducted by legally authorized distributors on e-commerce platforms. Game points can be spent either through direct credit card top-ups at the store or by purchasing game point cards and entering their serial numbers to load points into a user's account. These points are then used to acquire virtual items and equipment, unlock in-game dungeons, participate in *gacha* (random draws), and engage in various other activities.

Customers of the online gaming industry come from diverse social backgrounds and groups. Current game rating regulations in our country limit player age but do not restrict specific identities. According to the 2021 Taiwan Player Behavior Survey Key Report²⁵, online questionnaire results indicate that most gamers (44%) are general office workers without managerial positions. In criminal practice, whether for fraud or ML, offenders often resell game point serial numbers shortly after acquisition to rapidly convert illicit proceeds into cash. The end users who redeem these points, typically authentic game players, are often unaware third parties with no direct connection to the criminals. Thus, the identity or occupation information of online game players currently holds limited reference value.

Due to the anonymity and liquidity of game point cards, the most common criminal typology involves fraud groups luring victims through various scams to purchase game point cards and providing the card serial numbers, thereby acquiring fraud proceeds. Regarding ML through game point cards, common methods include the following:

(1) Proxy top-up/resale of game points

Criminals top-up or sell game point serial numbers purchased with illicit funds on other trading platforms (such as treasure trading sites) at prices slightly below official sale prices, converting illicit proceeds into legitimate income.

(2) Purchase and resale of virtual items/game currency

Criminals load game point cards purchased with illicit funds, buy virtual items or game currency in the game store, and then resell these through other trading platforms to other players.

(3) Distribution of game point cards

Fraud rings establish companies to purchase game points in bulk from point vendors and then sell them to general consumers overseas, laundering illicit proceeds as revenue from distributing game points.

In summary, the structure and business nature of the online gaming industry itself are not complex, but due to the anonymity and liquidity of game point cards, these products pose a relatively high ML risk compared with other business types within the industry. However, in the domestic context, the current market is dominated by mobile games, where a fast-paced

²⁵ Source: <https://www.gamerating.org.tw/Page?itemid=1&mid=53> (Last accessed: November 12, 2024)

gaming environment has led most players to shift their spending habits toward direct credit card top-ups, commonly known as in-app purchases. Sales of game point cards represent only a small portion of total game point revenue. Therefore, this assessment has adjusted the industry's risk rating from the previous "high" to "medium".

17. Medium-Risk Vulnerability: Securities Investment Trust Enterprises (including Futures Trust Enterprises)

| Assessment period | 2021 | 2024 |
|-------------------|-------------|---------------|
| Rating | High | Medium |

Securities investment trust enterprises (hereinafter referred to as SITEs) primarily conduct fundraising and sales activities (including public funds, private funds, and offshore funds) as well as discretionary investment management. As of the end of 2023, there were 38 such firms, of which 8 also operate futures trust enterprises (only three have issued futures trust funds), managing a total asset scale of NTD12.8 trillion. Compared with major domestic financial industries such as domestic banks and securities firms, SITEs are smaller. Fund sales are conducted either by the enterprises themselves or through financial institutions. Discretionary investment management is contracted directly with clients, who are required to deposit entrusted investment assets with custodian institutions (approved financial institutions). Most business relationships with clients are continuous and transactional in nature, characterized by a simple business structure that does not involve client cash flow, thereby resulting in an overall low level of business complexity.

The characteristics of SITEs do not allow for rapid movement of funds. Investors conducting fund transactions or discretionary investments must have their invested capital and fund usage handled through a custodian institution's designated accounts and cannot utilize the funds arbitrarily. Redemptions of funds or withdrawals of discretionary investment capital must also be processed through custodian institution designated accounts, which require a considerable amount of processing time; therefore, clients cannot use SITE products or services to rapidly move funds.

Fund sales are processed by the enterprises themselves or through financial institutions, while discretionary investments are contracted directly with clients who must have invested assets held by custodian institutions (approved financial institutions). Among the products provided by SITEs, private funds and discretionary investments tend to serve only a minority or specific clients due to product design, thus posing relatively high ML and FT risks compared with public funds. By the end of 2023, private funds and discretionary investments together accounted for approximately 22.67% of the total managed assets, while offshore funds accounted for 24.7%. The SITE industry remains predominantly driven by public funds.

Most transactions between SITEs and clients are continuous, with the majority of client relationships originating through financial institution sales channels. Direct customers account for a relatively small share of SITE's overall operations in terms of both client numbers and transaction volumes, thereby limiting direct interaction with high-risk clients. SITE clients are mainly natural persons, with only a small portion comprising legal persons, foreigners, and domestic and foreign PEPs. As of the end of 2023, corporate clients accounted for approximately 1.81%, foreign investors 0.077%, and domestic and foreign PEPs about 0.067%. Although SITEs have high-net-worth clients, their proportion is only about 0.387%, which is lower than that in the banking sector.

SITE business activities are conducted primarily within Taiwan. The company has only three overseas subsidiaries, and in 2023, investments in foreign assets accounted for 49.38% of its total assets. Clients and investment targets largely do not involve high-risk jurisdictions. Clients from jurisdictions of concern, such as the British Virgin Islands, Samoa, and the Cayman Islands, accounted for approximately 0.057% of total clients. Investments in China, Indonesia, Cayman Islands, Vietnam, Hong Kong, and the Philippines—also jurisdictions of concern—accounted for about 7.24% of total SITE-managed funds. Investments in high-risk jurisdictions accounted for about 1.317% of total SITE-managed funds.

The majority of transactions between SITEs and clients are conducted via sales channels through regulated financial institutions. As of 2023, a significant proportion of SITE sales clients placed orders online, with non-face-to-face transactions (including online, voice, fax, and written communications) accounting for approximately 89.87% of transaction counts, and electronic transactions (including online and voice) accounting for about 2.43% of transaction value.

Compared with the previous assessment, private funds and discretionary investment—both considered relatively higher-risk activities—account for only about 22.67% of SITEs’ assets under management and do not constitute the dominant portion of the business. In addition, the proportions of foreign and domestic PEP clients and high-net-worth individuals have also declined compared with the prior assessment. Accordingly, this risk assessment adjusts the industry’s overall risk rating from “high” to “medium”.

18. Medium-Risk Vulnerability: Foreign Migrant Worker Remittance Companies

| Assessment period | 2021 | 2024 |
|-------------------|------|--------|
| Rating | N.A. | Medium |

As of the end of December 2023, Taiwan had three foreign migrant worker remittance companies with total assets of NTD3.3 billion and operating capital of NTD1 billion, categorizing them as small-scale financial service providers. In 2023, income from overseas small-amount remittances of foreign migrant workers totaled NTD730 million, with a net operating profit of NTD360 million. As of the end of 2023, the total number of customers was 630,000. The total transaction amount for 2023 reached NT\$63 billion, with 6 million transactions conducted, resulting in an average transaction value of NT\$10,342 per transaction. The business of foreign migrant worker remittance companies is considered restricted. Customer identity, payment destination, and fund source are all subject to relevant regulations, and the business structure is simple, with relatively low integration with other industries.

These companies primarily provide services for foreign migrant workers in Taiwan, enabling them to remit wages back to their home countries. Remittance amounts are capped at NTD30,000 per transfer, NTD50,000 monthly accumulation, and NTD400,000 annually per remitter.

The customers of these companies are exclusively foreign migrant workers residing in Taiwan, specifically foreign nationals engaged in work specified under subparagraphs 8 to 11 under Paragraph 1 of Article 46 of the Employment Service Act and holding a resident certificate. There are no corporate customers or temporary transactions. There are 23,185 high-risk clients, accounting for 3.7% of the total customers, who are mostly engaged in manufacturing, construction, or household caregiving. They are not expected to maintain any client relationships with domestic or foreign PEPs or high-net-worth individuals.

Regarding the geographic scope of business activities, the source countries of this sector's clients and the beneficiary locations for outward remittances are highly concentrated in high-risk jurisdictions identified by the FATF, specifically the Philippines and Vietnam. Clients from these countries represent approximately 47.8% of the total, and transactions with these countries as remittance destinations account for about 50.4%, thereby reflecting a higher risk.

Clients of foreign migrant worker remittance companies establish business relationships exclusively through non-face-to-face methods using a mobile app, although they must still provide and upload relevant identification documentation for verification. Most clients prefer to pay remittance amounts at convenience stores, and complex service channels are rarely involved. Since most clients and transactions are handled through non-face-to-face methods, a certain level of risk remains.

In summary, foreign migrant worker remittance companies are classified as restricted businesses, with clear regulatory requirements for client identity, beneficiary location, fund source, and remittance amount. The industry does not serve corporate clients or conduct temporary transactions, so the overall risk should be limited. However, due to the sector's activities being highly concentrated in FATF-designated high-risk jurisdictions and the fact that most clients and transactions are processed through non-face-to-face means, these characteristics still represent certain risks. Therefore, the overall risk rating is "medium".

Chapter 7. Risk Assessment Results: Proliferation Financing Risk

In October 2020, the FATF revised Recommendation 1 and its interpretive notes, requiring all countries and private sector entities to identify, assess, understand, and mitigate the risk of PF. In light of FATF Recommendation 1 and the June 2021 publication of the “Guidance on Proliferation Financing Risk Assessment and Mitigation,” PF risk is strictly confined to the potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in Recommendation 7²⁶. As the requirements of Recommendation 7 apply to all UNSC resolutions relating to the proliferation of weapons of mass destruction and subsequent resolutions and are implemented according to the practices of specific countries, UNSC Resolution 1718 (2006)²⁷ and its subsequent resolutions apply to North Korea. As for Iran, the UN terminated the provisions of previous related resolutions in 2015 through UNSC Resolution 2231 (2015), implementing the Joint Comprehensive Plan of Action (JCPOA) while retaining certain targeted financial sanctions on designated individuals and entities. Accordingly, FATF Recommendation 7 requires all countries to freeze, without delay, funds or other assets and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of: 1. any individual or entity designated by the United Nations, 2. any individual or entity, acting on behalf of, or at the direction of, such designated individuals or entities, or 3. any individual or entity owned or controlled by such individuals or entities.

This risk assessment, in line with FATF requirements, primarily evaluates PF risks related to North Korea and Iran while also considering broader PF risks to enable a deeper and more comprehensive understanding and identification of the PF risk facing Taiwan.

Section 1. Proliferation Financing Threats

I. North Korea

In reviewing recent international developments, China, North Korea, and Russia have continued to deepen military and economic cooperation, engaging in trade involving petroleum, coal, and dual-use goods through both land and maritime routes. To evade export controls and law enforcement scrutiny, they employ methods such as third-country transshipment, front companies, concealment of end users, and alteration of customs data to create transaction cut-off points. North Korean oil tankers frequently conduct transactions in the Yellow Sea and East China Sea, often hiding their whereabouts by altering ship names, International Maritime Organization (IMO) numbers, transmitting false Maritime Mobile Service Identity (MMSI) signals, or disabling Automatic Identification Systems (AIS) to conduct covert dealings.

From 2021 to 2023, Taiwan’s enforcement authorities investigated several cases involving the provision of PF to North Korea. These cases typically involved nationals acting as responsible persons or ultimate controllers of shipping companies that declared the export of oil products by listing non-sanctioned countries as the destinations. In some cases, non-Taiwanese-flagged vessels using falsified names were found to be delivering oil to third-

²⁶ The private sector entities referred to here include financial institutions, designated DNFBPs, and VASPs.

²⁷ Guidance on Proliferation Financing Risk Assessment and Mitigation, <https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html> (Last accessed: November 12, 2024)

country ships via ship-to-ship transfers on the high seas or directly to waters near North Korean ports. These activities involved exporting petroleum to vessels linked to the North Korean regime, thereby not complying with United Nations resolutions related to counter-PF measures. The primary perpetrators are typically shipping company executives, vessel owners, crew members, or third-country corporations with connections to the North Korean authorities.

These actors commonly collude with foreign accomplices, use ships registered in other countries, or conduct transactions through third parties to evade regulations, demonstrating that Taiwanese offenders in PF cases have international networks and the ability to conduct cross-border transactions. Most oil transfers occur on the high seas; in recent years, there have been instances of direct deliveries to North Korean ports, which has increased the difficulty of evidence collection for Taiwanese law enforcement. It is estimated that proceeds from proliferation-related activities amount to at least several hundred million NTD.

II. Iran

Amid rising tensions in the Middle East, Iran has sought to develop weapons of mass destruction by employing multi-layered procurement networks—using intermediaries and front companies in third countries—to conceal end users and purchase strategic high-tech goods from Taiwanese suppliers. Foreign nationals from Iran, the United Arab Emirates (UAE), and other countries, as well as offshore companies, logistics providers, and Taiwanese importers/exporters, are considered high-risk individuals or entities for PF.

From 2021 to 2023, enforcement cases relating to illegal export to Iran primarily involved Taiwanese suppliers exporting strategic high-tech goods without the required permits, in contravention of the Foreign Trade Act. The exported goods principally included water purification equipment and components, vertical machining centers, vertical lathes, and electronic control devices. Perpetrators were mainly companies and sales personnel. The criminal method involves selling goods through normal commercial channels, but falsifying customs documents to list the export destination as a non-restricted area while actually shipping goods to Iran.

Due to U.S. sanctions on Iran, Taiwanese banks are prohibited from accepting remittances from Iranian clients. Consequently, trade is often facilitated through Turkish and UAE trading companies as fictitious counterparties, with funds remitted via Dubai or Türkiye to create disruptions in the financial flow. It is also common for export declarations to list Dubai trading companies as consignees, while goods are actually routed to Iran. Overall, Taiwan's exports are mainly to the United States, Japan, and Mainland China, with minimal exposure to high-risk jurisdictions. While some cases of unlicensed export of strategic high-tech goods to Iran have been detected, these remain isolated incidents. Offenders, although possessing cross-border trade capacity and third-country networks and logistics resources, are generally dealing with only a limited number of countries. It is estimated that illegal profits from proliferation-related activities amount to at least tens of millions of NTD.

Case Study

Mr. A, the de facto responsible person of Company A, knowingly sold and exported water purification equipment and component products—some of which are classified as “strategic high-tech goods” by Taiwan’s Ministry of Economic Affairs. These goods require prior approval and an export permit issued by the International Trade Administration of the Ministry of Economic Affairs before they can be shipped to controlled areas such as Iran. However, Mr. A, in order to profit from exporting these goods to Iran, colluded in using fictitious UAE consignee information provided by Iranian Company B to circumvent export controls and surreptitiously shipped goods to Iran. In 2021, prosecutors brought charges, and in 2022, the district court sentenced Mr. A to six months in prison.

Source: Investigation Bureau, Ministry of Justice

Section 2. Vulnerabilities in Proliferation Financing

I. Geographic and Environmental Factors

(1) North Korea

On September 22, 2017, in response to North Korea’s repeated missile launches and nuclear tests, which posed a serious threat to international order and national security, Taiwan announced a comprehensive ban on bilateral trade with North Korea. This action aligned with the international community’s consensus to uphold regional stability and order. Nevertheless, clandestine operations by private enterprises persist. According to the RUSI research report, Taiwan’s oil prices are among the lowest in East Asia. As a result, North Korea prefers to procure oil through affiliated actors in Taiwan, using tankers with clean records to facilitate export. The oil is then transferred via ship-to-ship operations in waters beyond Taiwan’s jurisdiction to other tankers destined for North Korea. In recent years, there have been several domestic cases of suspected illegal trade with North Korea, resulting in sanctions imposed either domestically or internationally.

The border between Mainland China and North Korea spans 1,420 kilometers. Both nations are governed by communist parties and maintain strict border controls, making access to Sino-Korean border regions highly restricted. Consequently, the transparency of related aid and trade activities is extremely low. Furthermore, the FATF mutual evaluation report on Mainland China, released in April 2019, rated Mainland China’s targeted financial sanctions against proliferation as “non-compliant” in technical compliance and “low level of effectiveness” in effectiveness ratings. Additionally, in 2023, Taiwan’s largest export market was Mainland China (including Hong Kong), accounting for 35.2% of total exports; the ASEAN-10 countries ranked second with 17.64%, followed by the United States at 17.63%, Japan at 7.27%, and the European Union at 8.51%. In the same year, Taiwan’s largest import source was Mainland China (including Hong Kong), accounting for 30.37% of total imports; the second-largest was Japan with 12.59%. ASEAN-10 countries accounted for 11.66%, the United States for 11.56%, and the European Union for 10.53%²⁸. These data indicate close economic and trade relations between Taiwan and Mainland China, necessitating special attention to the impact of Mainland China on PF issues facing our country.

²⁸ Source: https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=1374&pid=776523&dl_DateRange=all&txt_SD=&txt_ED=&txt_Keyword=&pageindex=1&history= (Last accessed: November 12, 2024)

(2) Iran

Taiwan does not share a land border with Iran, and related goods and personnel flows primarily depend on sea and air transportation. This reliance necessitates stringent border inspections to prevent potential loopholes in PF controls.

Some Middle Eastern countries tend to adopt a relatively lenient approach to regulating the flow of goods to Iran. Despite Iran being subject to U.S. economic sanctions and international courier services suspending shipments to the country, some private operators continued to provide mailing services destined for Iran. Additionally, although strategically controlled items exported from Taiwan to Middle Eastern nations do not declare Iran as the final destination, it is practically difficult to monitor whether these items are diverted to Iran indirectly.

II. Political and Social Factors

Taiwan has a strong political will to combat PF, making it a key priority on the national political agenda. In active cooperation with international efforts, Taiwan has taken concrete actions against PF, including the enactment and promulgation of the Counter-Terrorism Financing Act on July 27, 2016, which establishes regulations for targeted financial sanctions addressing the financing of terrorists, terrorism, and proliferation. Subsequently, to implement UNSC-related resolutions, the Council of Agriculture under the Executive Yuan (now reorganized as the Ministry of Agriculture) announced on May 12, 2017 a total ban on hiring North Korean crew members. The Ministry of Economic Affairs also announced a comprehensive ban on trade with North Korea on September 25, 2017, adopting the strictest control measures. Therefore, since 2018, Taiwan's import-export trade volume with North Korea has been zero, with no trade transactions. Moreover, to cooperate globally in preventing the proliferation of weapons of mass destruction, in addition to referencing the export control lists of the four major export control regimes—the Wassenaar Arrangement (WA), Missile Technology Control Regime (MTCR), Nuclear Suppliers Group (NSG), and Australia Group (AG)—our country has formulated the List of "Export Control List for Dual Use Items and Technology and Common Military List" and established "Sensitive Goods Lists" specifically for North Korea and Iran to strengthen export controls.

Regarding exchanges with North Korean and Iranian nationals, all such persons must apply for visas through our overseas diplomatic missions. Visas are issued only after these missions have reviewed and verified the legitimacy of the applicant's purpose for visiting Taiwan. Moreover, in line with announcements from the Central Epidemic Command Center, full resumption of visa facilitation and normal visa processing procedures took effect from October 13, 2022. Iranian nationals recommended by the Taiwan External Trade Development Council's local offices are eligible to apply for electronic visas.

III. Legal and Institutional Factors

(1) Relevant Laws and Regulations for Countering Proliferation Financing

1. Counter-Terrorism Financing Act.
2. Regulations Regarding the Operation of the Counter-Terrorism Financing Review Committee, Exceptional Measures for Sanctions, and Related Restrictions.
3. Directions for the Operations of the Investigation Bureau, Ministry of Justice, in Anti-Money Laundering and Counter-Terrorism Financing Practices.

4. Regulations on Anti-Money Laundering and Countering the Financing of Terrorism Operations for Financial Institutions and Designated Non-Financial Businesses and Professions.
5. Regulations Governing Anti-Money Laundering and Counter-Terrorism Financing Act for Specific Foundations, as Managed by the Competent Authority.

(2) Relevant Measures for Countering Proliferation Financing

In accordance with Paragraph 1 of Article 5 of the Counter-Terrorism Financing Act, individuals, legal persons, or groups designated under UNSC resolutions related to counter-terrorism financing and their subsequent resolutions, as well as those designated under UNSC resolutions concerning the prevention and suppression of the proliferation of weapons of mass destruction, shall be immediately designated by the Ministry of Justice as sanctioned parties. This demonstrates that domestic law already implements UNSC-related resolutions. If there is an update to the sanctions list announced by the UNSC, the Ministry of Justice shall immediately publish the corresponding updates in accordance with Article 5 of the Counter-Terrorism Financing Act. If the update involves any national, legal person, or group in Taiwan, their assets shall be frozen in accordance with the law. In 2018, a case arose in which a Taiwanese national was designated for sanctions by the UNSC, and Taiwan promptly announced the sanctions. Sanction lists are publicly accessible on designated sections of the Ministry of Justice and the Investigation Bureau websites, ensuring comprehensive implementation of UNSC sanctions resolutions.

With regard to targeted financial sanctions for PF, Articles 4 and 5 of the Counter-Terrorism Financing Act serve as the legal basis for designating individuals, legal persons, or groups for sanctioning. To date, one natural person and four legal persons have been designated under Article 4; the aforementioned individual was later delisted due to death. In addition, one national has been designated under Article 5 of the Act.

The Act stipulates procedures for designation, including the composition and convening of the Review Committee for Counter-Terrorism Financing, as well as the Regulations Regarding Committee Operations, Exceptional Measures, and Restrictions, which should be followed accordingly. Additionally, regarding the freezing of assets of beneficial owners, on November 7, 2018, Article 7 of the Counter-Terrorism Financing Act was revised to provide a legal basis, in compliance with FATF Recommendations 6 and 7. To date, both instances of designation have followed these procedures.

(3) Law Enforcement Capability to Counter Proliferation Financing

The Investigation Bureau of the Ministry of Justice is one of the main authorities responsible for investigating PF. Pursuant to Paragraph 12 under Article 2 of the Organizational Act of the Investigation Bureau, the Bureau is tasked with “domestic and foreign institutional coordination and liaison, international cooperation, investigation of national security cases involving foreign elements, as well as assisting with cross-border crime investigations” and is authorized to cooperate with foreign intelligence and national security agencies to investigate proliferation threats and coordinate related administrative or law enforcement agencies through special counter-proliferation initiatives.

Regarding international cooperation, due to diplomatic and political constraints, Taiwan has been unable to join the United Nations or participate in related meetings, nor has it entered into judicial mutual assistance agreements with most countries, resulting in limited avenues for international cooperation. Nonetheless, efforts are made to interact and share intelligence with

partnering foreign law enforcement officials, aiming to build expertise and experience necessary to investigate PF cases and to join the fight against proliferation activities. Currently, international partners are able to provide assistance and appropriate responses.

(4) Implementation of United Nations Embargoes or Other Measures

In terms of export trade, the International Trade Administration under the Ministry of Economic Affairs promptly incorporated the domestic sanctions list into the “Strategic High-Tech Commodities Export Entity Control List” and published it on its website, ceasing the issuance of export permits to listed entities. In 2017, a comprehensive ban on trade with North Korea was also announced. Strategic high-tech commodity export controls encompass a range of items, including dual-use goods, as well as sensitive goods destined for North Korea or Iran. The export entity control list is periodically submitted to the Customs Administration under the Ministry of Finance for coordinated border management.

For maritime and port matters, the Maritime and Port Bureau of the Ministry of Transportation and Communications enforces the sanctions list, complies with comprehensive bans on trade with North Korea under the Foreign Trade Act, and enacts or suspends import or export restrictions on specified countries, regions, or goods as necessary. It also distributes UNSC or international think tank reports on North Korea to relevant businesses and enforces port entry bans on specified vessels, including those sanctioned by the UNSC Sanctions Committee and other North Korea-related ships. Such notifications are issued to stakeholders and related agencies through official correspondence and website announcements.

On the customs front, the Customs Administration, in addition to cooperating with the implementation of the trade ban on North Korea and other administrative restrictions, has continued to issue notifications to the industry. It has also strengthened awareness within free trade zones regarding the rules governing high-seas transactions, and businesses have thus far demonstrated a high level of compliance.

IV. Economic and Technical Factors

(1) Virtual Asset Service Providers

On November 7, 2018, the Executive Yuan designated the Financial Supervisory Commission as the competent authority for AML supervision of enterprises handling virtual currency platform or transaction and defined the scope of such businesses on April 7, 2021. The Financial Supervisory Commission, drawing on FATF Recommendations, enacted and promulgated the “Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction” on June 30, 2021, requiring providers to conduct customer verification, maintain records, and file STRs as part of their AML and CFT efforts.

On July 31, 2024, Paragraph 2 under Article 5 of the Money Laundering Control Act was amended to replace “enterprises handling virtual currency platform or transaction” with “virtual asset service providers (VASPs)”, while Article 6 stipulates that those who have not completed AML registration with the central authority may not provide virtual asset services. VASPs established outside of Taiwan may not offer services domestically unless they register their company or branch pursuant to the Company Act and complete AML registration.

Currently, there are no concrete cases indicating that domestic PF actors have utilized VASPs to conduct PF activities. However, given that the current scale and profile of users of this industry within our borders is not fully understood and that international evidence,

including cases involving North Korea and other designated individuals and entities, has confirmed the use of virtual assets to circumvent sanctions, potential risk of such misuse persists.

(2) Control and Audit Mechanisms for Financial and Logistical Flows in Trade and Transshipment

The Bankers Association of the Republic of China has issued the “Guidelines for Banks Handling Settlement of Trade Payments with Iran,” requiring enterprises to submit relevant documentation and apply to the handling bank to process transactions. If a bank detects transactions with Iranian companies, organizations, or individuals listed on the control list or transactions in which these parties are the ultimate beneficial owners, the transactions will be rejected. However, since October 2018, the Taiwan–Iran funds settlement mechanism has ceased operations, and, in practice, banks are no longer processing related transactions. Currently, banks also reject all transactions involving North Korea. In accordance with Article 5 of the Foreign Trade Act, Taiwan imposed a comprehensive ban on trade with North Korea as of September 25, 2017; thus, there have been no financial dealings between the two parties.

With regard to the management and inspection mechanisms for strategic high-tech goods, export control is strengthened through the coordinated operation of visa processing by various visa-examining agencies, goods identification by the Industrial Technology Research Institute, pre- and post-audits by the International Trade Administration of the Ministry of Economic Affairs and its overseas offices, and implementation by intelligence agencies of coordinated operational approaches such as transnational intelligence cooperation and customs border control, thereby enhancing the export control of strategic high-tech goods.

(3) Marine or Cargo Insurance and Reinsurance Sectors

Currently, the insurance industry in Taiwan does not provide marine, cargo, or reinsurance coverage to businesses from North Korea and Iran. During the underwriting process, insurance companies do not direct funds to sanctioned entities and are required to review whether the vessel or aircraft to be insured is subject to sanctions. If it is a designated target, coverage will be denied. When coverage is granted, insurers will include special clauses excluding coverage for incidents involving international sanctions, and claims will not be paid if a sanctioned entity is involved. Additionally, because insurance claims can be processed only in the event of an incident specified in the policy and given the indemnity-based nature of property insurance—where policy periods are generally one year—the risk of PF through such insurance arrangements remains low.

(4) Other Financial Institution Services

There is a risk that accounts held by foreigners in Taiwan may be used for illicit financial transactions. Due diligence on such account holders, as well as imposing criminal sanctions on individuals outside our jurisdiction, presents certain challenges, thereby increasing the likelihood that these accounts could be used for illicit financing. Therefore, CDD and relevant risk mitigation measures by financial institutions and DNFBPs are of utmost importance for these types of clients. Appropriate measures should be considered to identify risks associated with accounts held by foreign nationals, citizens of high-risk jurisdictions, and diplomatic or embassy staff.

Moreover, correspondent banking business facilitates the international movement of funds, making it relatively difficult to obtain due diligence information on customers. Consequently, correspondent banking relationships present a higher risk of illegal financial activities.

Internationally, there have been cases in which PF networks exploited complex correspondent banking arrangements to undermine financial order across nations. Accordingly, financial institutions in Taiwan should pay special attention to these risks.

(5) Free Trade Zones

Taiwan currently has six seaport and one airport free trade zones: Keelung Port Free Trade Zone, Taipei Port Free Trade Zone, Su'ao Port Free Trade Zone, Taichung Port Free Trade Zone, Anping Port Free Trade Zone, Kaohsiung Port Free Trade Zone, and Taoyuan International Airport Free Trade Zone. Recent analysis of law enforcement investigations has found that perpetrators of several PF cases have used free trade zones to conduct fuel trading activities. Thus, increased vigilance and targeted mitigation efforts are warranted in these zones.

V. Legal Persons and Arrangements/Trusts

(1) Legal Persons

In November 2018, Taiwan amended the Company Act to add Article 22-1, requiring companies to report information on their responsible persons and major shareholders. In November 2018, the “Information Platform for Reporting Company Responsible Persons and Major Shareholders” was launched for companies to file their reports online. The current filing rate is about 90%, effectively increasing corporate transparency and providing information on beneficial ownership structures. Furthermore, through inquiry and anomaly reporting mechanisms available to financial institutions and DNFBPs, the accuracy of related information can be verified in a timely manner.

By utilizing the established “Information Platform for Reporting Company Responsible Persons and Major Shareholders”, major shareholder data can be obtained, further enhancing corporate transparency. Additionally, after a company files data via the aforementioned platform, mechanisms enabling financial institutions and DNFBPs to conduct inquiries and report anomalies ensure the accuracy of relevant information. Supplemented by subsequent verification by administrative authorities, this framework also ensures the accuracy, timeliness, and completeness of reported information.

As for limited partnerships, although there are currently no requirements for reporting beneficial ownership, the number of limited partnerships remains relatively low (as of May 2024, there were only 164). According to the Regulations Governing the Application of Limited Partnership Registration, registration authorities review and retain basic partner information, as well as related contract documents. Additionally, the names and capital contributions of general partners are publicly available online. If changes occur, a change in registration must be filed within the specified timeframe. This demonstrates that registration authorities can still track information about partners and their capital contributions.

(2) Legal Arrangements/Trusts

According to Paragraph 1 under Article 4 of the Trust Law, where property rights that are required to be registered are made the subject of a trust, the trust shall not be enforceable against third parties unless it has been duly registered as a trust. For example, in cases where ownership registration is required for real estate or marketable securities, the registration of trust property is conducted concurrently to establish enforceability against third parties.

In the case of civil trusts, the trustee's submission of trust property information and the settlor's or beneficiary's right to inspect, copy, or photocopy relevant documents are governed by Articles 31 and 32 of the Trust Act. Pursuant to these provisions, the trustee is required to maintain separate ledgers for each trust, detailing the status of trust affairs, and must prepare, at least once annually, an inventory of the trust property together with a statement of receipts and expenditures, which shall be delivered to the settlor and the beneficiaries. The settlor or beneficiaries may request to inspect, copy, or photocopy the aforementioned documents, and may further require the trustee to provide explanations regarding the administration of the trust. Interested parties may also request to inspect, copy, or photocopy these documents when necessary. Furthermore, pursuant to Paragraph 2 of Article 60 of the Trust Law, the court may, upon petition by interested parties or prosecutors, inspect trust affairs, appoint inspectors, and issue necessary orders.

The disclosure of the handling and financial status of public trusts is regulated under Article 72 of the Trust Law. The competent authority responsible for the public trust may inspect trust affairs and property status at any time. Trustees of public trusts must submit reports on trust management and financial conditions at least once annually to public trust supervisors for review, followed by submission to the competent authority for record and public announcement. Regarding the method of public disclosure of such trustee information, the regulations governing the approval and supervision of public trusts established by the competent authority, require that such information be published at the trustee's place of business and on information networks.²⁹

To address deficiencies identified in APG's third round of mutual evaluations, Taiwan has amended the Money Laundering Control Act to explicitly stipulate in Article 11 that non-trustees in the trust industry—limited to DNFBPs or other legal persons acting as trustees—must obtain and maintain adequate, accurate, and up-to-date identification information concerning the settlor, trustee, beneficiary, and any other natural persons with ultimate effective control over the trust. They must also maintain basic information on other trust agents and trust service providers.

Section 3. Proliferation Financing Risk Assessment Results

PF activities pose threats to regional security and socioeconomic stability. Although Taiwan's geographical environment and trade conditions are conducive to such activities—particularly proliferation activities involving North Korea—Taiwan's government has maintained foresight on this issue, striving not only to enhance domestic legal frameworks and systems but also to cooperate internationally to jointly combat PF.

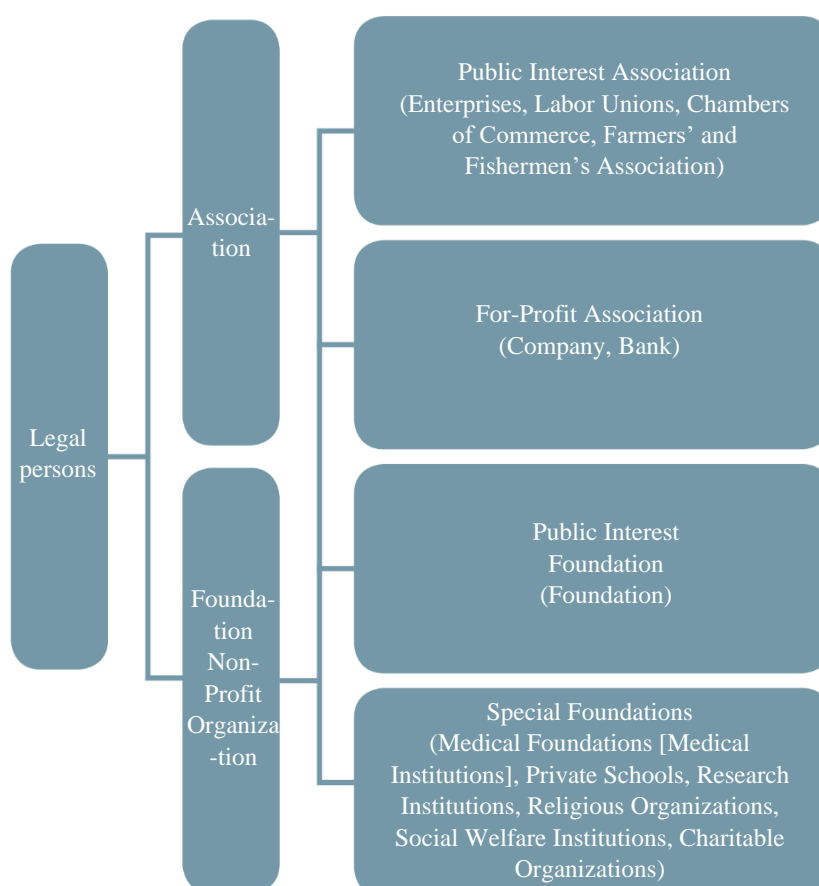
This risk assessment process has identified that Taiwan's PF threats mainly stem from activities involving North Korea. It has also recognized specific industries beyond financial institutions and DNFBPs that may participate in or be potentially exploited, such as maritime transport, ship leasing, customs brokerage, commodity suppliers, and the marine fuel industry. These sectors must heighten awareness of PF and remain vigilant regarding potential risks. Moreover, challenges remain regarding the transparency of legal persons and arrangements/trusts in identifying beneficial owners, with limited feedback from relevant public and private sectors. Therefore, continuous efforts should be made to enhance the understanding of their obligations among financial institutions, DNFBPs, and the aforementioned industries. Additionally, certain regulations and measures related to PF require further study and revision. Accordingly, Taiwan's overall PF risk assessment rates the North Korea-related risk as "Moderate" and the Iran-related risk as "Low".

²⁹ For relevant list contents, please refer to the Ministry of Economic Affairs' International Trade Administration Trade Information Network website: <https://www.trade.gov.tw>.

Chapter 8. Risk Assessment Results: Legal Persons

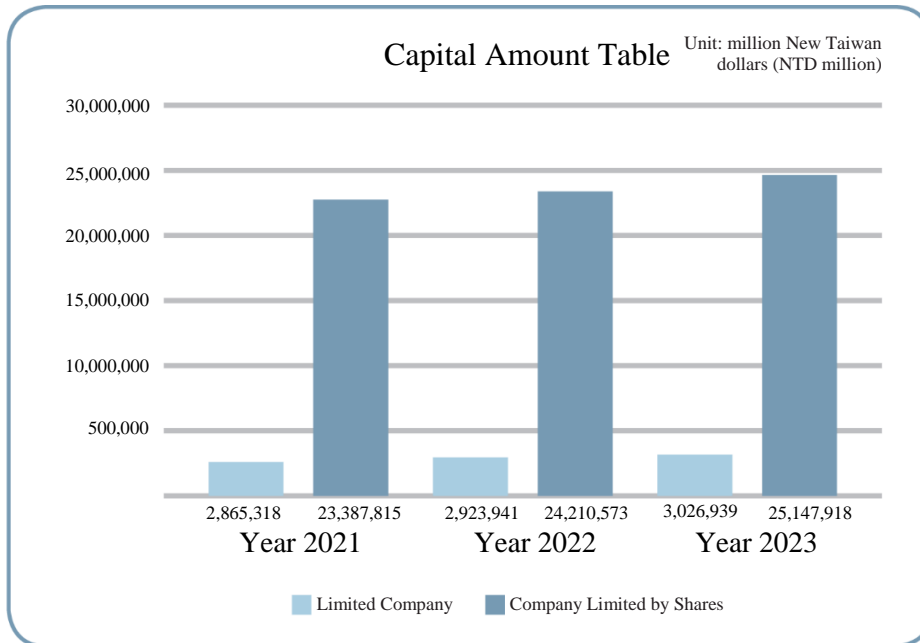
| Rating \ Type | Public Companies | Non-Publicly Listed Company | | | Limited Partnership |
|--------------------------|---------------------------|-----------------------------|-----------------|---|---------------------|
| | Company Limited by Shares | Company Limited by Shares | Limited Company | Unlimited Company & Unlimited Company with Limited Liability Shareholders | Limited Partnership |
| Previous Risk Assessment | Lower Risk | Higher Risk | Higher Risk | Lower Risk | Lower Risk |
| Current Risk Assessment | Lower Risk | Higher Risk | Higher Risk | Lower Risk | Lower Risk |

Legal persons in Taiwan are mainly classified into two major categories: associations and foundations. This chapter's risk assessment focuses on for-profit associations, namely, companies; other types are addressed in Chapter 10 concerning NPOs. Below is a schematic of the types of legal persons in Taiwan:



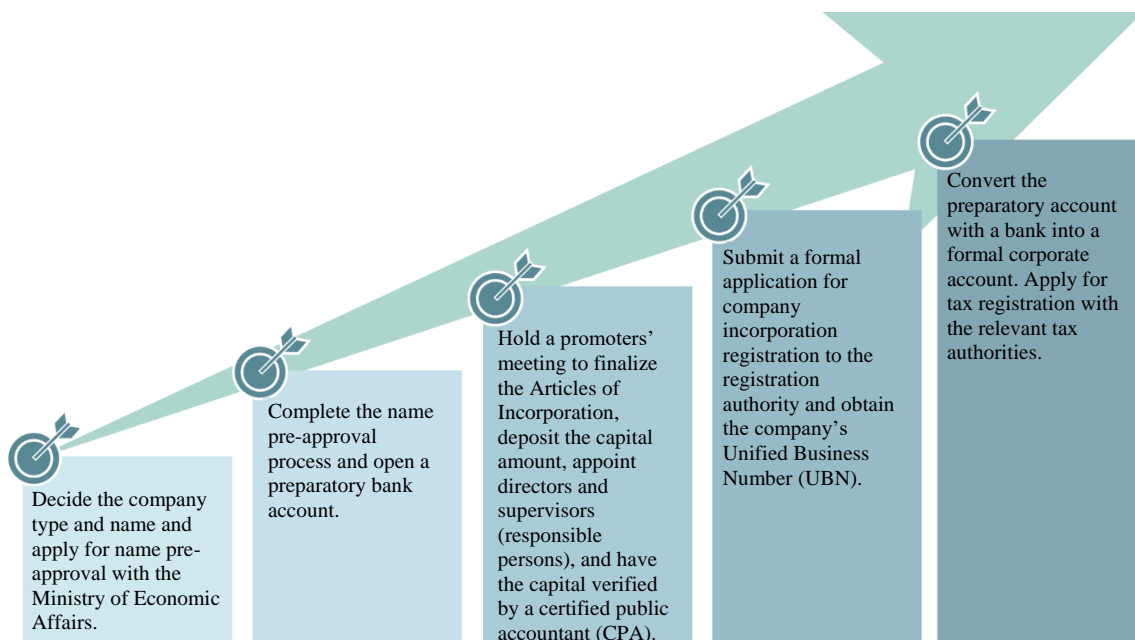
As of the end of 2023, the total number of registered companies was 771,311. Among them, Limited Companies accounted for the majority, totaling 578,810, followed by Companies

Limited by Shares, which numbered 186,836. There were 2,641 publicly listed companies and 184,195 non-publicly listed companies (including 5,434 close companies). The number of companies of all types increased compared with the previous risk assessment period. The capital of Limited Companies grew, as did that of Companies Limited by Shares, indicating an overall industry growth trend.



Taiwan applies a principle-based approach to company incorporation, with the registration authority conducting a formal review (see below for the company incorporation registration procedure flowchart).

Company Incorporation Registration Procedure Flowchart



Company incorporation or registration of changes does not impose mandatory agency or dedicated proxy systems; however, if a proxy is appointed, the agent must be a CPA or a lawyer

(proxy usage ratio illustrated below). In practice, due to cost and complexity considerations, small companies often engage consulting firms, bookkeeping professionals, or bookkeeping and tax agents to assist with registration procedures, even if they do not appoint a proxy. Furthermore, when establishing a company or increasing capital, the capital contribution must be inspected by a CPA. For companies with capital exceeding NTD30 million, the financial statements are required to be attested by a CPA. In practice, companies may directly entrust a CPA to handle capital structure planning, capital verification, and registration matters, as well as manage company registration-related items.

Statistics of company registration cases handled by CPAs and lawyers in the past three years:

| Agent | Statutory Agent | | | | Non-Statutory Agent: Self-managed or Appointed Proxy | | Total | |
|-------|---------------------------------|----------------------|--------------------|----------------------|--|----------------------|--------------------|----------------------|
| | Certified Public Accountants | | Attorneys | | | | | |
| Year | Number of Cases | Annual Proportion | Number of Cases | Annual Proportion | Number of Cases | Annual Proportion | Number of Cases | Annual Proportion |
| 2023 | 123,765 | 23.10% | 3,257 | 0.61% | 408,859 | 76.30% | 535,881 | 100.00% |
| 2022 | 119,955 | 22.94% | 3,354 | 0.64% | 399,690 | 76.42% | 522,999 | 100.00% |
| 2021 | 113,369 | 21.43% | 2,834 | 0.54% | 412,803 | 78.03% | 529,006 | 100.00% |

Regarding the geographical scope of industry activities, Taiwan is primarily a trade-dependent economy, with its trade-to-GDP ratio reaching 108.33%. As for jurisdictions of concern, in 2023, Taiwan's top five trading partners by trade value were Mainland China at USD165.9 billion, the United States at USD116.8 billion, Japan at USD75.7 billion, Hong Kong at USD58 billion, and South Korea at USD46.6 billion. In terms of high-risk jurisdictions, according to the list of high-risk jurisdictions published by the FATF in October 2023: 1. High-Risk Jurisdictions Subject to a Call for Action: North Korea, Iran, and Myanmar. 2. Jurisdictions under increased monitoring: including Barbados, Bulgaria, Burkina Faso, Cameroon, Democratic Republic of the Congo, Croatia, Gibraltar, Haiti, Jamaica, Mali, Mozambique, Nigeria, the Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Türkiye, Uganda, UAE, Vietnam, and Yemen. As of 2023, Taiwan engaged in trade with all of these jurisdictions, with the exception of North Korea. For example, in 2023, Taiwan's top five high-risk FATF jurisdictions in trade were Vietnam (approximately USD17.8 billion), the Philippines (about USD7.41 billion), the UAE (about USD5.13 billion), Türkiye (about USD1.82 billion), and South Africa (about USD1.81 billion).

With respect to suspicious transaction reports, the number of company-related STRs disseminated by the Financial Intelligence Unit between 2021 and 2023 was as follows (where the company could be the perpetrator or the victim): 1,540 in 2021, 1,065 in 2022, and 903 in 2023. Among these, the predominant types of suspected criminal activities were in non-compliance with of the Company Act, fraud, insider trading, market manipulation, embezzlement, and securities fraud.

Analysis of cases handled by law enforcement in recent years indicates several key ways companies have been misused for criminal purposes:

I. Setting up shell companies or using existing companies to commit predicate offenses and launder money, for example:

- (1) Company insiders collude with external parties to fabricate sham transactions, enabling the transfer of company assets, falsification of financial statements, or submission of fake purchase and sales invoices to tax authorities, in order to facilitate embezzlement, fraudulent fundraising, stock price manipulation, or tax evasion. The illicit proceeds are then moved through company accounts for ML purposes.

- (2) Using the company name to recruit staff, establish business premises, or open accounts, then conducting illegal fundraising, underground banking, telecom fraud, or online gambling, with illicit funds subsequently laundered through company accounts.

Case 1

Person A, the responsible person of Company A, together with his sister, who served as the company's accountant, accepted requests at Company A's place of business from other companies, such as Company B, to conduct RMB currency exchanges. The sister instructed these clients to remit equivalent amounts of NTDs into designated financial institution accounts domestically. They would then cash a Company A check in mainland China for the RMB equivalent and transfer the funds to the clients' designated accounts in Mainland China. These activities constituted the illegal operation of an NTD-RMB remittance business between Taiwan and Mainland China.

Source: Taiwan High Prosecutors Office

Case 2

Person A, a wanted criminal with gang affiliations, used his father's name as chairman to set up a company offering real estate financing and matchmaking services, including second mortgage loans and note trading. The company's executives frequently appeared in photos with high-ranking politicians and allegedly used images of senior journalists for promotional purposes while allegedly raising illegal funds. The platform promised high returns, employing schemes such as "fake debt, real fundraising" and "using new funds to pay old returns", attracting tens of thousands of investors. From early 2021, the platform began to default, failing to repay the principal amount, and suddenly stopped paying interest in late April 2023.

Source: Taiwan High Prosecutors Office

II. Mainland Chinese (PRC) or foreign-invested enterprises establishing subsidiaries in Taiwan to steal trade secrets

These crimes often involve PRC enterprises legally establishing local subsidiaries and utilizing various channels and opportunities to acquire key technologies from Taiwan's high-tech sector.

Case Study

Person A established Company A in Mainland China and invited Person B, employed by Company B, to work at Company A to assist in setting up Company A's Taiwan R&D department. Individual B, intending future employment at Company A, took unauthorized photographs of business secrets belonging to Company B using a mobile phone and then reproduced the photographed files onto a laptop provided by Company A. From September 2020, he leased an office in Hsinchu County to establish Company A's Taiwan R&D department. In November 2020, Person A further hired Individual C, who, without authorization, forwarded confidential business files to their private email, reproduced the trade secrets of Company C and Company D, copied these confidential files onto a USB drive connected to their private laptop, and subsequently transferred the reproduced trade secret files onto laptops or desktop computers provided by Company A, thereby stealing trade secrets.

Source: Taiwan High Prosecutors Office

High-risk crimes potentially involving legal persons include fraud, smuggling, tax offenses, insider trading and market manipulation, as well as corruption and bribery. Among these, some foreign companies established in tax havens and offshore financial centers, although not registered in Taiwan, are set up by nationals through management consulting firms or are directly established overseas. Criminals exploit these channels, often in conjunction with the use of OBU accounts, to carry out illicit activities.

Current data indicate that due to Taiwan's prosperous economic and trade development, the scope of company industry activities is broad, with a high proportion involving jurisdictions of concern. Among company types, companies limited by shares and limited companies constitute the majority of registrations. Law enforcement experience indicates that due to insufficient transparency, non-publicly listed companies—specifically, companies limited by shares and limited liability companies—are the most commonly abused types. Associated sectors potentially involved include accounting firms, law firms, and bookkeeping professionals providing services during the incorporation process. Publicly listed companies have information disclosure obligations and must publish important financial and operational information on platforms such as the Market Observation Post System (MOPS). Therefore, publicly listed companies possess a certain degree of transparency, characterized by higher levels of information disclosure. Furthermore, publicly listed companies listed on stock exchanges are subject to stringent requirements, including verification and disclosure procedures for material information, thereby ensuring even higher transparency. Hence, the likelihood of publicly listed companies being exploited for criminal purposes is lower than that of non-publicly listed companies. As for unlimited company with limited liability shareholders, unlimited company, and limited partnerships, given their smaller capital and total sales as well as fewer instances, criminal exploitation is extremely rare, resulting in a lower risk.

In February 2022, FATF strengthened Recommendation 24, requiring jurisdictions to assess the risk of legal persons being abused for ML or FT. According to the FATF Recommendation 24 guidance on Beneficial Ownership of Legal Persons³⁰, the risks of ML and FT should be identified and assessed for the following four categories of foreign legal persons with substantial connections to Taiwan:

1. Foreign legal persons with a permanent establishment, branch, or office in Taiwan

From 2021 to 2023, the number of foreign companies establishing branches in Taiwan was 364, 333, and 334, respectively. The number of registrations entrusted to accountants was 222, 205, and 207, respectively. The number of registrations entrusted to lawyers was 39, 48, and 30, respectively.

From 2021 to 2023, the number of foreign companies establishing offices in Taiwan was 347, 301, and 241, respectively. The number of registrations entrusted to accountants was 138, 129, and 102, respectively. The number of registrations entrusted to lawyers was 14, 12, and 11, respectively.

³⁰ <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf> (Last accessed: November 12, 2024)

2. Foreign legal persons with significant business activities in Taiwan

From 2021 to 2023, the operating capital of foreign companies' branches in Taiwan was NTD12,893,338,917, NTD3,679,529,531, and NTD2,275,477,884, respectively, showing a declining trend year over year.

Furthermore, from 2021 to 2023, the total number of foreign companies' branches and offices in Taiwan holding tax identification numbers, along with their total sales amounts, is detailed as follows. Statistical data indicate that, except for 2021, when the sales volume of foreign offices in Taiwan was notably higher, the overall scale of business activities remained largely unchanged during the risk assessment period. Additionally, the business scale of foreign companies' branches in Taiwan was significantly larger than that of foreign offices.

Total Sales of Foreign Companies' Branches and Offices Holding Tax Identification Numbers in Taiwan

Unit: NTD

| | Foreign Companies' Branches in Taiwan | Foreign Companies' Offices in Taiwan |
|-----------------------------|---------------------------------------|--------------------------------------|
| Total Sales Revenue in 2021 | 1,916,220,842,090 | 2,432,787 |
| Total Sales Revenue in 2022 | 2,122,249,831,216 | 267,514 |
| Total Sales Revenue in 2023 | 1,771,062,825,181 | 303,969 |

Total Number of Foreign Companies' Branches and Offices Holding Tax Identification Numbers

Unit: Number of Cases

| | Foreign Companies' Branches in Taiwan | Foreign Companies' Offices in Taiwan |
|-----------|---------------------------------------|--------------------------------------|
| Year 2021 | 11,769 | 105 |
| Year 2022 | 12,126 | 105 |
| Year 2023 | 12,476 | 105 |

3. Foreign Legal Persons Having Significant and Ongoing Business Relationships with Taiwan's Financial Institutions

(1) Banking Sector

From 2021 to 2023, the total number of deposit accounts opened by foreign legal persons in our country's OBUs was 129,036, 126,369, and 124,733, respectively, with total deposit balances amounting to NTD100,997,249,516, NTD114,326,158,011, and NTD109,921,549,303.

From 2021 to 2023, the total number of deposit accounts opened by foreign legal persons in our country's domestic banking units (DBUs) was 12,636, 12,615, and 12,868, respectively, with total deposit balances amounting to NTD384,865,171,438, NTD505,783,827,643, and NTD411,209,400,341, respectively.

(2) Insurance Sector

Insurance products are generally divided into two major categories: life insurance and property insurance. Among life insurance products, life insurance and annuity insurance possess policy reserve values. From 2021 to 2023, the proportion of foreign legal persons purchasing life insurance among all insurance customers (including life and property insurance) was 4.12%, 3.73%, and 2.95%, respectively. Their premium expenditure correspondingly accounted for just 17.64%, 17.14%, and 14.53% of total premium expenditure. This indicates that foreign legal persons primarily purchase property insurance. Among the premiums paid, life insurance and annuity insurance combined represented only 10.13%, 9.37%, and 6.58% of the total premiums paid by foreign legal persons from 2021 to 2023, respectively, showing a relatively low share with a decreasing trend.

(3) Securities Sector

As of the end of 2021, 2022, and 2023, the approximate number of active securities accounts held by foreign legal persons in our country was 9,375, 10,028, and 10,544, respectively. The market value of listed stocks held was NTD19.96 trillion, NTD14.10 trillion, and NTD18.73 trillion, respectively, accounting for 32.17%, 28.95%, and 29.9% of the total market capitalization of listed companies.

4. Foreign Legal Persons Owning Real Estate or Other Investments Domestically

As of July 12, 2024, a total of 604 foreign legal persons had acquired real estate in our country, comprising 1,543 parcels of land and 1,664 buildings, mostly located in municipalities (accounting for approximately 90%). The total publicly announced land value was about NTD43.8 billion.

Chapter 9. Risk Assessment Results: Legal Arrangements/Trusts

| Item \ Risk Assessment | Business Trust | Public Trust | Civil Trust |
|--------------------------|----------------|--------------|-------------|
| Previous Risk Assessment | Lower Risk | Lower Risk | Higher Risk |

| By Type of Trustee | | |
|--|----------------|--------------------|
| Item \ Risk Assessment | Business Trust | Non-Business Trust |
| Current Risk Assessment | Lower Risk | Higher Risk |
| Classified by Purpose of Trust Establishment | | |
| Item \ Risk Assessment | Public Trust | Private Trust |
| Current Risk Assessment | Lower Risk | Higher Risk |

According to Article 1 of the Trust Law, a “trust” refers to a legal relationship in which a settlor transfers or otherwise disposes of property rights, requiring the trustee to manage or dispose of the trust property in accordance with the trust’s purpose for the benefit of the beneficiaries or for a specific purpose. In Taiwan, trusts can be categorized as “business trusts” or “non-business trusts” based on whether the trustee is an institution engaged in the trust business. Alternatively, trusts can be divided into “public trust” or “civil trust” based on their purpose of establishment. As for the supervisory authorities of trusts, they differ depending on the nature of the trust: business trusts are supervised by the Financial Supervisory Commission, while public trusts fall under the jurisdiction of the competent authorities for their respective purposes.

Business trusts refer to trusts established by trust enterprises for business purposes. Trust enterprises are institutions licensed by the competent authority to engage in the trust business under the Trust Enterprise Act. Non-trust enterprises may not accept trust business commissioned by an indefinite number of people. Services encompassed by business trusts include money trusts; trusts in monetary claims and their collateral; securities trusts; trusts in movable and immovable property; trusts in lease rights, superficies rights, patent rights, copyrights, and other property rights. Currently, trusts in Taiwan are primarily business trusts. There are no dedicated trust enterprises in Taiwan, and most trust businesses are operated concurrently by financial institutions, including banks, securities firms, credit cooperatives, and agricultural banks. Additionally, while settlors of trust property may include high-net-worth individuals, professionals in cash-intensive industries, or individuals domiciled in high-risk jurisdictions for ML or FT, their proportion remains relatively low. Financial institutions operating trust businesses must be licensed by the Financial Supervisory Commission in accordance with the Trust Enterprise Act and must comply with AML disclosure requirements

applicable to financial institutions. They are also subject to heightened supervision by the FSC. Accordingly, the level of information transparency is relatively high, so the current risk assessment remains low.

Non-business trusts are those accepted by trustees for purposes other than business, such as trusts in which private individuals, lawyers, or accountants serve as trustees. Essentially, simply signing a trust contract only has legal effect under the law of obligations; however, as stipulated by the Trust Law, the transfer of property that requires registration or recording as trust property may not be asserted against third parties unless the trust is registered. Thus, when the trust property involves real estate, securities, or similar assets requiring ownership registration, trust property registration provides relative transparency of information. Nevertheless, non-business trusts may be established verbally or in writing, and access to information about the ultimate beneficial ownership behind the trust assets remains limited, thereby impeding in-depth risk assessments for ML and FT purposes. Furthermore, current Taiwanese regulations concerning “non-business trusts” are primarily derived from the Trust Law, yet the Law does not sufficiently address the requirements for trustee disclosure and reporting of trust property. Accordingly, non-business trusts carry a higher risk compared with business trusts.

A public trust is defined as a trust established for philanthropic, cultural, academic, artistic, religious, ancestral worship, or other public interest purposes. Given that the total assets of public trusts represent a very small share overall, their business activities are straightforward and uncomplicated, and operations are limited to domestic activities without involvement in high-risk ML/FT jurisdictions. Additionally, both settlors and beneficiaries are clearly recorded, ensuring transparency of information. Moreover, trustees of public trusts are mainly financial institutions, with trust business subject to FSC supervision. On this basis, public trusts are deemed to present lower risk compared with private trusts.

The FATF revised Recommendation 25 in February 2023, requiring countries to assess the ML and FT risks associated with legal arrangements and to adopt mitigating measures. According to Paragraph 3 of the Interpretation Note to FATF Recommendation 25, countries should assess legal arrangements with the following characteristics: “Countries should assess ML/FT risks associated with all types of trusts and other similar legal arrangements—(a) those governed under domestic law; (b) those administered domestically or for which the trustee or equivalent holds residence domestically; and (c) types of foreign legal arrangements with sufficient links to Taiwan—and take appropriate measures to manage and mitigate identified risks.” The aforementioned “sufficient links” to the country include instances where “the foreign legal arrangement and the trustee or its equivalent maintain substantial and ongoing business relationships with Taiwan’s financial institutions or DNFBPs, hold significant real estate or other investments domestically, or are tax residents domestically.”³¹ Based on the above FATF definition, regarding (a) “governed under domestic law,” i.e., domestic trusts, the risk assessment has been discussed as above. For (b) and (c), i.e., foreign legal arrangements, the explanation is as follows:

I. Banking Sector

From 2021 to 2023, the total number of deposit accounts opened for trust assets by foreign trusts under trustees other than trust enterprises was 11, 9, and 7, respectively, with total deposit balances of approximately NTD41.31 million, NTD39.39 million, and NTD66.35 million.

³¹ The FATF Recommendations, www.fatf-gafi.org/recommendations.html (Last accessed: November 12, 2024).

Banks handle the opening of dedicated trust asset accounts in accordance with the Bankers Association’s “Guidelines for Trustees Other Than Trust Enterprises to Apply for Trust Asset Accounts at Financial Institutions” and the “Regulations Governing Anti-Money Laundering of Financial Institutions.” The requirements are as follows: 1. both the settlor and trustee must provide dual identification documents, as well as a “notarized trust deed,” with verification that the trust relationship is genuine. 2. The settlor and trustee must complete an account opening declaration form and provide relevant information and photocopies of identification documents for “the trust supervisor, trust beneficiary(ies), and any other person who can effectively control the trust account, or persons holding equivalent or similar positions as the aforementioned parties.” 3. If the trustee is not a natural person, the trustee must also provide relevant information and copies of identification documents for the “beneficial owner” and “senior management personnel”. When a customer applies to open an account, the bank must review and understand the customer’s intended operating model. If the customer indicates involvement of a trust structure, the bank must request the standard documents as well as the trust deed and have the customer explain the trust structure to obtain information on the settlor, trustee, and beneficiaries.

| Item | 2021 | 2022 | 2023 |
|---|------------------|------------------|------------------|
| Total deposit balances for deposit accounts opened in the name of non-trust enterprise trustees of foreign trusts | NTD41.31 million | NTD39.39 million | NTD66.35 million |
| Number of deposit accounts opened in the name of non-trust enterprise trustees of foreign trusts | 11 accounts | 9 accounts | 7 accounts |

Source: Financial Supervisory Commission

II. Securities and Futures Industry

There are currently no relevant statistical data on the total assets in trust accounts or the number of clients for foreign trust customers. However, pursuant to Subparagraph 2 of Article 3, Item 3 of Subparagraph 4, Item 2 of Subparagraph 7, and Subparagraph 3 of Article 5 of the Regulations Governing Anti-Money Laundering of Financial Institutions (“AML Regulations”), financial institutions, when establishing a business relationship with a customer, must verify the customer’s identity and identify the customer’s beneficial owner(s). They must also take reasonable measures to verify these identities, including the use of reliable data sources or other credible information. Where a customer is acting as the trustee of a trust, the financial institution must verify the identities of the settlor, trustee, trust supervisor, trust beneficiary(ies), and any other persons who can effectively control the trust account, or those holding equivalent or similar positions. Financial institutions are required to conduct ongoing due diligence on customer identities, periodically review whether the information obtained for identifying customers and beneficial owners is adequate, and ensure that such information is kept up-to-date, especially for high-risk customers, for whom reviews must be conducted at least once per year. Accordingly, when a foreign trust establishes a business relationship with domestic securities or futures firms, those firms should be able to obtain relevant information regarding the settlor, trustee, and beneficiary.

III. Certified Public Accountants

According to Subparagraph 2 and Item 3 under Subparagraph 3 of Article 7 of the Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Certified Public Accountants, when establishing a business relationship with a client, accountants must verify the client's identity, identify the client's beneficial owner(s), and take reasonable measures to verify their identities, including via the use of reliable sources of data or information. According to Subparagraph 4 of the same article, Subparagraph 3 requires when a client acts as the trustee of a trust, accountants must understand the nature of the client's or trust's business, including any similar legal arrangements, and obtain relevant information to identify and verify the client's identity. Under Subparagraph 5 of the same article, as further provided in Item 3 of Subparagraph 3, accountants must also understand the ownership and control structure of the client or trust, identify the beneficial owner(s), and take reasonable measures to verify their identities. In addition, Subparagraph 2 of Article 9 of the same Regulations requires accountants to conduct ongoing CDD throughout the business relationship, including periodic reviews to ensure that information obtained for identifying clients and beneficial owners remains adequate and up to date. For high-risk clients, such reviews must be conducted at least annually.

IV. Land Administration Agents and Real Estate Brokerage Industry

According to statistics from the Department of Land Administration, Ministry of the Interior, as the current system cannot filter registered property data for designated legal owner over a specific period, only cadastral data at the time of inquiry can be provided. During the period covered by this risk assessment, foreign legal persons acquired three parcels of land and four buildings via trust arrangements; the total publicly announced value of the land acquired by foreign legal persons via trusts was approximately NTD79.45 million. To ensure the security of real estate transactions and protect consumer rights, land administration agents and real estate brokers shall verify the identity of clients or their agents prior to accepting engagement, and the Department of Land Administration, as the competent authority, requires supervision in accordance with Article 8 of the Regulations Governing Anti-Money Laundering and Counter-Terrorism Financing for Land Administration Agents and Real Estate Brokerages—for any real estate transaction where the act is carried out by the trustee of a trust or when property rights are assigned to a third party, the identities of the legal entity client, the trustee, supervisor, beneficiary, or third party must be verified in order to identify the natural person(s) with ultimate effective control and the relevant identification data must be retained or recorded. Additionally, Taiwan employs a written, real-name registration system for real property title transfers. Under land registration regulations, when a foreign branch applies for land title registration, it shall register in the name of the foreign company (i.e., the head office), with the responsible person in Taiwan serving as the applicant and submit the branch establishment (or change) registration form, transcript, or certified copy issued by the competent company registration authority, together with the foreign company establishment (or change). However, the registration authority does not obtain identification information on the ultimate beneficial owner(s).

V. Others

No domestic property or life insurance company has underwritten insurance policies for foreign trust clients. For the legal profession, there are currently no statistics on foreign trust clients or the total value of trust property. Additionally, from 2021 to 2023, no instances have been identified involving the acceptance of income tax returns for trust property or for offshore trust entities.

In summary, Taiwan currently lacks comprehensive oversight of statistical information related to foreign legal arrangements/trusts. When trustees do not voluntarily disclose their status, identifying the parties to the trust becomes challenging. This results in a high degree of privacy and, consequently, a relatively elevated risk of abuse for ML and FT—an issue that warrants continued attention from the authorities.

Chapter 10. Risk Assessment Results: Non-Profit Organizations

NPOs in Taiwan are categorized by their attributes as either civil associations or foundations, with competent authorities being the Ministry of the Interior, the Ministry of Health and Welfare, the Ministry of Education, the Ministry of Culture, and municipal governments. According to the FATF Recommendation 8 classification, NPOs are further divided by nature into categories such as cultural, religious, social/fraternal/charitable, medical, and educational. This risk assessment focuses primarily on nationwide NPOs as their operations span the entire country, making their activity scope broader and their degree of foreign interaction and complexity higher.

NPOs carry risks of misuse for FT; however, given that terrorist financing risk is low in Taiwan, this assessment targeted the six main types of NPOs as defined by the FATF, evaluating ML and FT risks. For rating purposes, a simplified identification and assessment method was used, classifying organizations into “higher risk” and “lower risk” categories. Organizations rated as higher risk include civil associations, nationwide religious foundations, and social welfare foundations. The following provides a breakdown of the risk rating for each type.

| Type Rating | Civil Associations | Nationwide Religious Foundations | Social Welfare Foundations | Medical Foundations | Educational Foundations | Cultural Foundations |
|--------------------------|--------------------|----------------------------------|----------------------------|---------------------|-------------------------|----------------------|
| Previous Risk Assessment | Higher Risk | Higher Risk | Higher Risk | Lower Risk | Lower Risk | Lower Risk |
| Current Risk Assessment | Higher Risk | Higher Risk | Higher Risk | Lower Risk | Lower Risk | Lower Risk |

Section 1. Higher-Risk Non-Profit Organizations

I. Civil Associations

Civil associations are organizations established based on “people”, and their operations and expenditures must be approved by the general assembly or the board of directors and supervisor, operating through a collective decision-making process. Civil associations include social associations and professional associations. Among them, social associations are organizations composed of individuals or groups that promote public interest through cultural, academic, medical, health, religious, charitable, sports, fellowship, social service, or other purposes; professional associations are formed by units, groups, or practitioners from the same industry or profession to coordinate industry relationships, enhancing mutual interests and advancing socioeconomic development. As of the end of December 2023, there were 24,118 registered national social associations and 477 registered national professional associations.

The revenues of civil associations include member contributions and other donations. Member contributions are voluntarily given by individuals or entities (such as corporations) who become individual or organizational members upon approval by the board of directors. These contributions are typically irregular in both frequency and amount. Other donations are made after the organization completes legal-person registration and applies to the competent

authority to conduct fundraising activities in accordance with the Public Welfare Solicitation Act and the Regulations for Permission of Public Welfare Solicitation. The funds and property obtained through such fundraising activities must be used in accordance with the utilization plan approved by the competent authority, may not be diverted for other purposes, and are subject to the supervision of the competent authority. In addition, under current laws and regulations, civil associations must submit their financial statements for approval by the general assembly (or the assembly of member representatives) before filing them with the competent authority for record. However, since filing with the authority serves only as a notification and there is no registration or public disclosure of the association's total assets, financial transparency for civil associations remains limited, posing a potential risk.

Concerning international activities, organizations such as the “Junior Chamber International Taiwan”, “Lions Clubs International Taiwan”, “Taiwan District of Kiwanis International”, “Taiwan Rotary Clubs Association”, and the “Red Cross Society of the Republic of China (Taiwan)” are chapters of international non-governmental organizations and are national social associations with higher degrees of involvement in global affairs. In addition to exchanges with various countries, some associations also interact with Mainland China, and several individual sports associations participate in competitions of International Olympic Committee member countries/regions. Consequently, international engagement is more frequent.

In summary, given the frequency of international activities and the incomplete implementation of financial transparency, civil associations are overall assessed as higher-risk NPOs.

II. National Religious Foundations

National religious foundations are established to promote spiritual teachings, foster moral development, and carry out related public welfare, charitable, and educational activities. As of the end of December 2023, there were 201 national religious foundations in operation, with a total registered asset value of NTD152,361,428,392. Among these, there were 89 Christian foundations with a combined asset value of NTD71,862,406,318; 39 Catholic foundations with NTD30,924,822,990; 42 Buddhist foundations with NTD26,996,011,335; 6 Taoist foundations with NTD1,162,677,810; and 25 foundations representing other religions with NTD21,415,509,939 in assets. Over the past three years, the total assets of national religious foundations have increased by more than NTD11.7 billion. Notably, the “Christian Chinese Faith, Hope & Love Foundation”, “Chung Tai Shan Buddhist Foundation”, “The Church of Jesus Christ of Latter-day Saints Taiwan Foundation”, “Seventh-day Adventist Church Taiwan Conference Foundation”, and “Tien En Maitreya Buddhist Institute Foundation” are national religious foundations with comparatively higher total registered assets.

Of all national religious foundations, only 71 were established through cash donations; the vast majority declared real estate assets, such as church buildings, temples, and other religious venues, as their primary registered property. Donation sources are mainly individuals (congregants), with a minority from private enterprises and foreign/domestic legal persons (often the contributing parent organization), as well as widely dispersed anonymous donations.

The primary activities of national religious foundations are conducted domestically, although a few engage in overseas activities in countries such as Cambodia³² and others. The foundations most frequently engaged in international affairs include the “Dharma Drum Mountain Buddhist Foundation”, “Taiwan Morrison Christian Association”, and “Jehovah's Witnesses Taiwan”.

³² From 2021 to 2022, Cambodia remained listed by the FATF as an “other country or jurisdiction with strategic deficiencies in AML/CFT compliance.”

In summary, considering the presence of anonymous donations among national religious foundations and the involvement of some with high-risk jurisdictions, these organizations are generally rated as higher-risk NPOs.

III. Social Welfare Foundations

National social welfare foundations (hereinafter referred to as “social welfare foundations”) are established for the purpose of promoting social welfare-related services. Their activities include services for women, children and youth, persons with disabilities, older persons, family support, social assistance, social work, volunteer services, domestic violence prevention, sexual assault prevention, and sexual harassment prevention. As of the end of December 2023, there were 326 social welfare foundations in operation with a total registered asset value of NTD189,905,104,000. Donation sources include the general public, groups, private enterprises, and other legal persons. The five largest social welfare foundations in terms of assets are the “Tzu Chi Foundation”, “VIA Faith, Hope & Love Charity Foundation”, “Taipei Jen Chi Home”, “Tainan Jen Ai Home”, and “Ching Pao Kin Lao Social Welfare Charity Foundation”.

The activities of social welfare foundations are mainly domestic, with only 2 retaining overseas offices, accounting for about 0.5% of the total. Additionally, some social welfare foundations operate overseas programs and services, including in Mainland China. Among the five social welfare foundations with the highest level of international involvement, three provide services in Myanmar, while others extend their activities to countries such as Vietnam and the Philippines. The more internationally engaged foundations include the “Buddhist Compassion Relief Tzu Chi Foundation”, “Taiwan Fund for Children and Families”, “Eden Social Welfare Foundation”, “World Vision Taiwan”, and “Zhi-Shan Foundation Taiwan”.

In summary, since some foundations extend their overseas services to high-risk jurisdictions such as Myanmar, Vietnam, and the Philippines, they are overall assessed as higher-risk NPOs.

Section 2. Lower-Risk Non-Profit Organizations

I. Medical Foundations

Medical foundations refer to foundations that operate medical institutions to provide healthcare services. They must obtain approval from the central competent authority and register with the court. In addition, they are permitted to operate affiliated facilities such as nursing homes, psychiatric rehabilitation centers, medical research institutes, and other welfare organizations as authorized under relevant laws, including the Senior Citizens Welfare Act. As of the end of December 2023, there were 53 medical foundations, with 52 in operation and one inactive. The total registered assets of these 53 medical foundations amounted to NTD201,687,570,881. The five largest medical foundations by registered assets are as follows: “Chang Gung Medical Foundation”, “Buddhist Tzu Chi Medical Foundation”, “Changhua Christian Hospital Medical Foundation”, “Cathay Medical Foundation”, and “Hsu Yuanzhi Medical Foundation”.

According to Paragraph 1 of Article 34 of the Medical Care Act, medical juridical persons must establish an accounting system based on the calendar year and the accrual basis, maintain accurate supporting documents for all financial transactions, keep necessary accounting records, follow generally accepted accounting principles, and ensure proper record retention. Paragraph 2

requires medical juridical persons to submit annual financial statements, approved by the board of directors and acknowledged by supervisors, to the central competent authority within five months after the close of the fiscal year. Therefore, there are no uncommon or anonymous donations, nor are there funds originating from high-risk jurisdictions. Funding sources predominantly comprise donations of cash, stocks, real estate, and similar assets. The scope of activities is mainly domestic, with no operations in high-risk jurisdictions.

II. Educational Foundations

Educational foundations are mainly of two types: “school foundations”, which refer to private schools at all levels (including universities and secondary schools) regulated by the Ministry of Education under the Private School Act, and “educational foundations”, which are established for public welfare purposes to support education, youth development, sports, or academic research activities and are supervised by the Ministry of Education or affiliated agencies under the Civil Code and Foundation Act.

As of the end of December 2023, organizations under the jurisdiction of the Ministry of Education included 201 school foundations with total registered assets of about NTD743,667,139,945 and 776 educational foundations with total registered assets of about NTD97,212,666,925. Among school foundations, the two with the highest registered assets are “China Medical University Foundation” and “Taipei Medical University Foundation”; among educational foundations, “Chang Yung-Fa Foundation” and “Ming-Wei Education Foundation” hold the highest total assets.

Donors are mostly domestic legal entities, organizations, and natural persons. School foundations disclose donations in accordance with Article 39 of the University Act. Educational foundations must accept donations under the foundation’s name for public welfare purposes and disclose this information as required by Article 26 of the Foundation Act. Anonymous contributions are relatively uncommon, and most donations do not reach the threshold for currency transaction reporting.

The geographical range of educational foundations’ activities is predominantly domestic. Only a few NPOs, such as Ming Chuan University, which has a U.S. campus, and the “Chiang Ching-kuo Foundation for International Scholarly Exchange”, operate internationally across the Americas, Europe, and the Asia-Pacific regions.

III. Cultural Foundations

Cultural foundations are established to foster the development of arts and culture and organize related events. As of the end of December 2023, the 196 foundations registered under the Ministry of Culture had a total registered asset value of NTD36,633,033,788. In addition to government-funded foundations, private donors are predominantly individuals in the local arts and culture community dedicated to supporting and advancing arts and culture. Most donations originate from domestic enterprises (legal entities) and natural persons, with relatively few donations from foreign legal entities or individuals. Among the 196 foundations supervised by the Ministry of Culture (including those established with government funding and private donations), 12 foundations have government contributions exceeding 50%, with a total registered asset value of NTD17,583,904,987.

The scope of activity for cultural foundations is primarily domestic. When international activities do occur, they are mostly limited to low-risk countries such as Japan, Europe, and the United States. Donors are domestic enterprises (legal persons) and individuals, with no donors

originating from high-risk jurisdictions. Entities with significant involvement in international affairs include the “Cultural Taiwan Foundation”, the “Asian Cultural Council Taiwan Foundation”, and the “Sheen Chuen-Chi Cultural and Educational Foundation”.

Cultural-type foundations primarily provide services through open and transparent channels, such as online platforms or public physical announcements; the use of complex or anonymous service channels is rare. Donations must comply with domestic regulations, and annual financial reports are submitted to the Ministry of Culture for record keeping.

Chapter 11. National Strategy and Future Plans

Viewed across the evolution of Taiwan's AML/CFT/CPF regime, the country moved from being the first jurisdiction in Asia to enact a dedicated anti-money laundering law, to subsequently being placed on APG's "enhanced follow-up" list during the mutual evaluation process, and has also endured significant sanctions imposed on a domestic bank by foreign supervisory authorities. At present, Taiwan has attained one of the strongest assessment outcomes within the APG and is now classified placed in the "regular follow-up" category. The process "from failing to leading Asia" has been built on countless efforts by both the public and private sectors, thus enabling a transparent and orderly financial environment. In the area of national risk assessment, Taiwan has accumulated experience from two previous National Risk Assessment reports, laying a solid foundation for a risk-based approach to combating ML, FT, and PF.

2018



For the first time, a national-level risk assessment of ML and FT was conducted to identify predicate offense threats and sectoral vulnerabilities, forming the basis for strengthening and revising enforcement and supervisory measures.

2021



The methods and scope of implementation are updated and adjusted as needed, such as adding assessment items, expanding participating agencies and personnel, enhancing domestic and international data collection, and, for the first time, conducting risk assessments on PF.

Learning from the past to guide the future, Taiwan's progress in AML/CFT/CPF will not stall simply because of positive results. In an era in which financial services and technology evolve rapidly, complacency could quickly cause us to fall behind international standards and the shifting risk landscape. Therefore, to further advance AML/CFT/CPF policy development, Taiwan completed its latest National Risk Assessment in 2024. Led by the Executive Yuan's Anti-Money Laundering Office, all relevant competent authorities participated in a comprehensive risk analysis at both the national and sectoral levels. The national risk assessment results, together with findings from the third round of APG mutual evaluations and the latest amendments to the FATF 40 Recommendations, were incorporated into a national AML/CFT/CPF strategy, outlining four strategic objectives and nine key focus areas.

I. Enhance the government's effectiveness in combating illegal financial activities

- (1) Continue promoting legal reform to increase the deterrent effect on criminals.
- (2) Ensure that government agencies have the tools, technologies, and support needed to disrupt illegal financial activities.
- (3) Enhance judicial agencies' capabilities to combat illegal financial activities.

II. Improve the supervision and enforcement effectiveness of financial institutions and DNFBPs

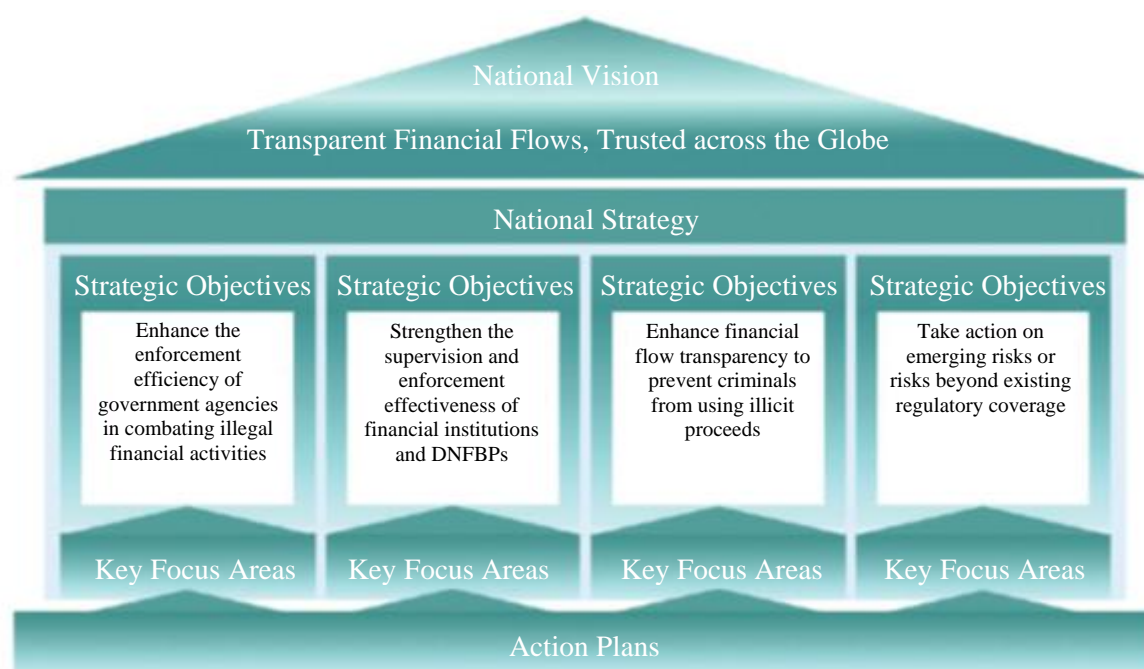
- (1) Strengthen due diligence to prevent criminals from directly or indirectly holding significant equity, control rights, or management positions.
- (2) Revise AML/CFT/CPF-related laws and measures for financial institutions and DNFBPs to align with international standards.
- (3) Continuously improve the capability to identify suspicious activities and enhance the efficiency of financial intelligence reporting.
- (4) Establish risk-based supervision plans to ensure allocation of more resources to high-risk areas.

III. Increase the transparency of financial flows to prevent criminals from using illicit proceeds

Enhance the acquisition, retention, and disclosure of information on legal persons and arrangements/trusts, improving the government's access to beneficial ownership information

IV. Take action on emerging risks or risks beyond existing regulatory coverage

Continue applying more targeted preventive measures to address trends in predicate offenses



To achieve the above four main strategic objectives, Taiwan is progressively implementing corresponding action plans in key areas and will regularly monitor, review, and revise their effectiveness as needed. Among these, strengthening the supervision and enforcement effectiveness of DNFBPs will be a top priority. In addition to aligning various DNFBP regulations with international standards, the effectiveness of their implementation will face more stringent scrutiny. This will also be a key focus in the upcoming APG fourth-round

mutual evaluation. Additionally, Taiwan will further enhance the collection and analysis of information on foreign legal persons and arrangements/trusts to improve the current transparency of beneficial ownership, which remains inadequate.

Taiwan will continue to refine AML, CFT, and CPF measures, deepen public-private sector cooperation, and respond more effectively to the risks of ML, FT, and PF, thereby fulfilling its duties and responsibilities as a global citizen. The Anti-Money Laundering Office of Executive Yuan will also continue to plan and promote national risk assessments and action plans, support the public and private sectors in implementing a risk-based approach, and work toward achieving the vision of “Transparent Financial Flows, Trusted across the Globe”.

Annex 1: Taiwan's Legal Framework for AML/CFT/CPF

Anti-Money Laundering–Related Regulations

Laws

1. Money Laundering Control Act (amended and promulgated on July 31, 2024)
[International Cooperation-Related Laws]
2. Law of Extradition (amended and promulgated on July 4, 1980)
3. Act to Implement United Nations Convention against Corruption (promulgated on May 20, 2015)
4. Law in Supporting Foreign Courts on Consigned Cases (promulgated on April 25, 1963)
5. Mutual Legal Assistance in Criminal Matters Act (promulgated on May 2, 2018)
6. Act Governing Relations between the People of the Taiwan Area and the Mainland Area (amended and promulgated on June 8, 2022)
7. Act Governing Relations with Hong Kong and Macau (amended and promulgated on January 12, 2022)
8. Tax Collection Act (amended and promulgated on December 17, 2021)
[Law Enforcement-Related Laws]
9. Criminal Code of the Republic of China (amended and promulgated on July 31, 2024)
10. Code of Criminal Procedure (amended and promulgated on July 31, 2024)
11. Fraud Crime Hazard Prevention Act (promulgated on July 31, 2024)
12. Human Trafficking Prevention Act (amended and promulgated on June 14, 2023)
13. Trademark Act (amended and promulgated on May 24, 2023)
14. Waste Disposal Act (amended and promulgated on June 14, 2017)
15. Anti-Corruption Act (amended and promulgated on June 22, 2016)
16. Child and Youth Sexual Exploitation Prevention Act (amended and promulgated on August 7, 2024)
17. Firearms, Ammunition, and Knives Control Act (amended and promulgated on January 3, 2024)
18. Customs Anti-Smuggling Act (amended and promulgated on May 9, 2018)
19. Narcotics Hazard Prevention Act (amended and promulgated on May 4, 2022)
20. The Smuggling Penalty Act (amended and promulgated on June 13, 2012)
21. Administrative Penalty Act (amended and promulgated on June 15, 2022)
22. Customs Act (amended and promulgated on May 11, 2022)
23. Police Power Exercise Act (amended and promulgated on April 27, 2011)
24. The Administrative Execution Act (amended and promulgated on February 3, 2010)

-
25. The Compulsory Enforcement Act (amended and promulgated on May 29, 2019)
 26. The Communication Security and Surveillance Act (amended and promulgated on July 31, 2024)
 27. Organized Crime Prevention Act (amended and promulgated on May 24, 2023)
 28. Trade Secrets Act (amended and promulgated on January 15, 2020)
 29. National Security Act (amended and promulgated on June 8, 2022)
 30. Copyright Act (amended and promulgated on June 15, 2022)
 31. Pharmaceutical Affairs Act (amended and promulgated on January 31, 2018)
 32. Public Officials Election and Recall Act (amended and promulgated on June 9, 2023)
 33. Presidential and Vice Presidential Election and Recall Act (amended and promulgated on June 9, 2023)
 34. Cultural Heritage Preservation Act (amended and promulgated on November 29, 2023)
 35. Forestry Act (amended and promulgated on May 5, 2021)
 36. Soil and Water Conservation Act (amended and promulgated on November 30, 2016)
 37. Slopeland Conservation And Utilization Act (amended and promulgated on January 9, 2019)
 38. Water Act (amended and promulgated on November 29, 2023)
 39. Water Pollution Control Act (amended and promulgated on June 13, 2018)
 40. Air Pollution Control Act (amended and promulgated on August 1, 2018)
 41. Fisheries Act (amended and promulgated on December 26, 2018)
 42. Act on Wildlife Conservation (amended and promulgated on January 23, 2013)
 43. Passport Act (amended and promulgated on January 20, 2021)
 44. Penal Act of Offenses Against National Currency (amended and promulgated on June 29, 2011)

[Laws Related to Preventive Measures – Financial Aspect]

45. Banking Act of The Republic of China (amended and promulgated on June 28, 2023)
 46. Agricultural Finance Act (amended and promulgated on January 18, 2017)
 47. Act Governing Bills Finance Business (amended and promulgated on December 5, 2018)
 48. Credit Cooperatives Act of the Republic of China (amended and promulgated on January 31, 2018)
 49. Act Governing Electronic Payment Institutions (amended and promulgated on January 19, 2023)
 50. Offshore Banking Act (amended and promulgated on December 28, 2016)
 51. Foreign Exchange Control Act (amended and promulgated on April 29, 2009)
 52. Financial Technology Development and Innovative Experimentation Act (promulgated on January 31, 2018)
 53. Postal Remittances and Savings Act (amended and promulgated on January 29, 2014)
 54. Securities and Exchange Act (amended and promulgated on August 7, 2024)
 55. Futures Trading Act (amended and promulgated on June 28, 2023)
 56. Securities Investment Trust and Consulting Act (amended and promulgated on June 28, 2023)
-

-
57. Insurance Act (amended and promulgated on November 30, 2022)
 58. The Central Bank of the Republic of China (Taiwan) Act (amended and promulgated on January 8, 2014)
 59. Trust Enterprise Act (amended and promulgated on January 31, 2018)

[Laws Related to Preventive Measures – Non-Financial Aspect]

60. Attorney Regulation Act (amended and promulgated on June 9, 2023)
61. Certified Public Accountant Act (amended and promulgated on January 31, 2018)
62. Notary Act (amended and promulgated on April 3, 2019)
63. Land Administration Agent Act (amended and promulgated on January 27, 2021)
64. Real Estate Brokerage Management Act (amended and promulgated on January 27, 2021)

65. Certified Public Bookkeepers Act (amended and promulgated on May 4, 2022)

[Laws Related to Transparency of Legal Persons, Trusts, and Non-Profit Organizations – Non-Financial Aspect]

66. Civil Code (amended and promulgated on January 20, 2021)
67. Company Act (amended and promulgated on December 29, 2021)
68. Trust Law (amended and promulgated on December 30, 2009)
69. Civil Associations Act (amended and promulgated on February 8, 2023)
70. Limited Partnership Act (promulgated on June 24, 2015)
71. Medical Care Act (amended and promulgated on June 28, 2023)
72. Private School Act (amended and promulgated on June 18, 2014)
73. Public Welfare Solicitation Act (amended and promulgated on January 15, 2020)
74. Foundations Act (promulgated on August 1, 2018)

Legal Orders and Administrative Rules

[Legal Orders and Administrative Rules Related to International Cooperation]

75. Cross-Strait Joint Crime-Fighting and Judicial Mutual Assistance Agreement (promulgated on April 26, 2009)

[Legal Orders and Administrative Rules Related to Law Enforcement]

76. Anti-Money Laundering Regulations for Cross-border Declaration and Reporting (amended and promulgated on November 4, 2022)
77. Regulations on the Management, Allocation, and Use of Property Confiscated from Money Laundering Crimes (promulgated on July 28, 2004)
78. Directions for Controlled Delivery in Customs Drug Enforcement (amended and promulgated on June 14, 2013)

[Legal Orders and Administrative Rules – Financial Aspect]

79. Regulations Governing Anti-Money Laundering of Financial Institutions (amended and promulgated on December 14, 2021)
 80. Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Securities and Futures Business and Other Financial Institutions Designated by the Financial Supervisory Commission (promulgated on November 9, 2018)
 81. Regulations Governing Anti-money Laundering of Agricultural Financial Institutions (amended and promulgated on December 27, 2018)
-

-
82. Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions (amended and promulgated on August 20, 2014)
 83. Directions Governing Banking Enterprises in Conducting Foreign Exchange Business (amended and promulgated on January 19, 2022)
 84. Regulations Governing Foreign Exchange Business of Banking Enterprises (amended and promulgated on January 28, 2021)
 85. Regulations Governing Postal Remittances and Savings Operations (amended and promulgated on January 8, 2019)
 86. Regulations Governing the Establishment and Administration of Foreign Currency Exchange Counters (amended and promulgated on January 26, 2022)
 87. Rules Governing Offshore Banking Branches (amended and promulgated on May 22, 2017)
 88. Regulations Governing Identity Verification Mechanism and Transaction Amount Limits of Electronic Payment Institutions (amended and promulgated on June 30, 2021)
 89. Regulations Governing Anti-Money Laundering of Financial Leasing Enterprises (promulgated on June 20, 2018)
 90. Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Financial Leasing Enterprises (promulgated on November 9, 2018)
 91. Regulations Governing Small Amount Remittance Services for Foreign Migrant Workers (promulgated on June 30, 2021)
 92. Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries (amended and promulgated on September 23, 2021)
 93. 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 (amended and promulgated on December 14, 2021)
 94. Regulations Governing Foreign Bank Branches and Representative Offices (amended and promulgated on December 29, 2022)
 95. Regulations Governing Institutions Engaging in Credit Card Business (amended and promulgated on October 13, 2021)
 96. Regulations Governing Qualification Requirements and Concurrent Serving Restrictions and Matters for Compliance by the Responsible Persons of Banks (amended and promulgated on April 13, 2023)
 97. Regulations Governing the Qualifications and Election/Appointment of Membership Representatives, Directors, Supervisors and Managerial Officers of Credit Cooperatives (amended and promulgated on October 26, 2020)
-

-
98. Regulations Governing Qualification Requirements and Concurrent Serving Restrictions and matters for Compliance by the Responsible Persons of a Specialized Electronic Payment Institution (promulgated on June 30, 2021)
 99. Regulations Governing the Responsible Persons and Business Staff Members of Bills Houses (amended and promulgated on October 26, 2020)
 100. Regulations Governing Internal Audit and Internal Control System of Anti-money Laundering and Countering Terrorism of Agricultural Financial Institutions (promulgated on December 27, 2018)
 101. Regulations Governing the Suspension or Closure of Account Functions for Accounts under Article 15-2, Paragraph 6 of the Money Laundering Control Act (promulgated on February 29, 2024)

[Legal Orders and Administrative Rules Related to Preventive Measures – Non-Financial Aspect]

102. Regulations on Anti-Money Laundering & Countering the Financing of Terrorism Operations Matters Conducted by Attorneys (amended and promulgated on October 15, 2021)
103. Guidelines for Attorneys on Anti-Money Laundering Obligations (promulgated on June 28, 2017)
104. Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Certified Public Accountants (promulgated on December 24, 2020)
105. Regulations Governing Anti-Money Laundering and Counter-Terrorism Financing for Land Administration Agents and Real Estate Brokerages (amended and promulgated on June 21, 2021)
106. Regulations Governing Anti-Money Laundering and Counter-Terrorist Financing for Certified Public Bookkeepers and Bookkeeping and Tax Return Filing Agents (amended and promulgated on December 22, 2021)
107. Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Jewelry Businesses (amended and promulgated on April 26, 2021)
108. Regulations Governing Anti-Money Laundering and Counter-Terrorism Financing for Notaries (amended and promulgated on October 28, 2024)
109. Standards for Determining the Scope of Politically Exposed Persons Entrusted with Prominent Public Function, Their Family Members and Close Associates (amended and promulgated on October 16, 2018)
110. Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction (promulgated on June 30, 2021)
111. Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises or Persons Providing Third-Party Payment Services (amended and promulgated on January 22, 2024)

[Legal Orders and Administrative Rules Related to the Transparency of Legal Persons, Trusts, and Non-Profit Organizations – Non-Financial Aspect]

-
112. Regulations on Disposal of the Financial Affairs of Social Associations (amended and promulgated on November 28, 2022)
 113. Regulations for the Permit and Registration Procedures of Social Associations (amended and promulgated on May 22, 2020)
 114. Guidelines for the Ministry of the Interior's Review and Supervision of the Establishment of National Religious Foundations (amended and promulgated on July 8, 2021)
 115. Ethical Management Regulations for National Educational Foundations (amended and promulgated on August 21, 2024)
 116. Directions Governing Codes of Ethical Practice for National Social Welfare Foundations (amended and promulgated on March 21, 2024)

Regulations Related to Countering Terrorism Financing and Proliferation Financing

Laws

1. Counter-Terrorism Financing Act (amended and promulgated on November 7, 2018)
2. The National Intelligence Law of the Republic of China (amended and promulgated on January 15, 2020)
3. Immigration Act (amended and promulgated on June 28, 2023)
4. Civil Aviation Act (amended and promulgated on June 28, 2023)
5. Statute Governing Issuance of R.O.C. Visas in Foreign Passports (amended and promulgated on January 22, 2003)
6. Foreign Trade Act (amended and promulgated on December 25, 2019)

Legal Orders and Administrative Rules

7. Regulations Governing the Operation of Terrorism Financing Prevention Review Committee and the Sanction Measures and Restrictions (promulgated on September 14, 2017)
8. Regulations Governing Reporting on the Properties or Property Interests and Locations of Designated Sanctioned Individuals or Entities by Financial Institutions (amended and promulgated on November 14, 2018)
9. Regulations Governing Agricultural Financial Institutions' Reporting on the Property, Property Interests and Location of the Property and Property Interests of the Designated Individual, Legal Person or Entity (amended and promulgated on December 27, 2018)

Annex 2: Competent Authorities for AML/CFT/CPF in Taiwan

| Agency Name | Tasks and Duties Related to AML/CFT/CPF | Total Budget (Unit: NTD1,000) |
|--|--|---|
| Anti-Money Laundering Office, Executive Yuan | Responsible for coordinating national AML, CFT, and CPF policies and implementation strategies; conducting national risk assessments; and overseeing and coordinating APG mutual evaluation country reports, on-site evaluations, and external liaison matters. | 2021: 20,005 2022: 17,700 2023: 27,252 |
| Ministry of Justice | Responsible for formulating national policies and legislation on AML, CFT, and CPF; establishing prosecutorial policies for law enforcement agencies; promoting international criminal justice cooperation; and acting as the competent authority for the legal profession. Relevant internal departments include the Department of Prosecutorial Affairs, the Department of International and Cross-Strait Legal Affairs, and the Department of Legal Affairs. Prosecutors' offices at all levels serve as the primary criminal investigation bodies. They are authorized to direct judicial police agencies in investigating all predicate offenses, as well as ML, FT, and PF offenses. | 2021: 1,700,423 2022: 1,685,440 2023: 1,957,327 |
| Judicial Yuan | As the highest judicial authority in Taiwan, it is responsible for judicial policy statistical analysis of trial data across all levels of courts. It directly supervises the Supreme Court, High Courts, and the Intellectual Property and Commercial Court. It also oversees the regulation and supervision of notaries. Internal divisions include the Civil Department and the Criminal Department. Additionally, courts at all levels are responsible for adjudicating all predicate offenses, ML offenses, and FT offenses. | 2021: 3,757,615 2022: 3,653,472 2023: 3,704,270 |
| Investigation Bureau, Ministry of Justice | Taiwan's criminal investigation and intelligence agency, responsible for safeguarding national security and preventing crime, investigates major crimes, economic crimes, ML, and FT offenses. Key internal units include the Economic Crime Prevention Division, the Agency Against Corruption, the Drug Abuse Control and Prevention Division, and the International Affairs Division. Additionally, the National Security Division is responsible for planning, guiding, coordinating, investigating, and evaluating counter-terrorism and counter-proliferation initiatives. | 2021: 5,713,290 2022: 6,106,176 2023: 6,633,568 |

| Agency Name | Tasks and Duties Related to AML/CFT/CPF | Total Budget (Unit: NTD1,000) |
|---|--|--|
| Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice | Serves as Taiwan's Financial Intelligence Unit (FIU), responsible for policy research and legislation related to AML and CFT; the receipt, analysis, processing, and dissemination of suspicious transaction reports, currency transaction reports, and declarations cross-border transportation of currency or bearer negotiable instruments by travelers or crew members; as well as items transported for money-laundering purposes through cargo shipments, express delivery, postal services, or other similar means; coordination and liaison on AML matters; and engagement in international cooperation, including participation in organizations and meetings, intelligence exchange, and joint investigations of transnational ML cases. | The budget is integrated with the Investigation Bureau, Ministry of Justice. |
| Agency Against Corruption, Ministry of Justice | Responsible for implementing anti-corruption and corruption prevention activities and investigating corruption offenses and related ML activities. | 2021: 469,274 2022: 462,247 2023: 539,359 |
| Administrative Enforcement Agency, Ministry of Justice | Responsible for the compulsory enforcement of public monetary obligations under the law. Handles the disposition (sale) of confiscated items entrusted by prosecutorial authorities in accordance with the law. | 2021: 1,529,421 2022: 1,524,402 2023: 1,578,980 |
| National Police Agency, Ministry of the Interior | As one of Taiwan's primary law enforcement agencies, its core duties include safeguarding national security, maintaining public order, and protecting critical infrastructure. It is also responsible for investigating organized crime, gambling, fraud, drug offenses, and related ML activities. Under its jurisdiction, the Criminal Investigation Bureau serves as Taiwan's main liaison with INTERPOL and comprises divisions such as the Investigation Section, Anti-Gangster Section, Drug Enforcement Center, Fraud Investigation Center, Economic Crimes Section, and INTERPOL Affairs Section. Additionally, the Security Division and Protective Security Division handle intelligence gathering related to FT cases. | 2021: 21,717,548 2022: 22,452,426 2023: 24,529,660 |
| National Immigration Agency, Ministry of the Interior | As one of Taiwan's law enforcement agencies, it is responsible for managing national border security, administering matters related to foreign nationals, and preventing human trafficking. Its duties include overseeing border entry and exit security; collecting, integrating, and investigating immigration information; probing human trafficking and related illegal activities; and facilitating international cooperation and intelligence sharing on transnational crimes. | 2021: 4,444,524 2022: 4,627,926 2023: 5,009,552 |
| Coast Guard Administration, Ocean Affairs Council | Responsible for maintaining the safety of Taiwan's maritime areas and coastline; investigating smuggling cases in maritime, coastal, estuarine, and non-commercial port areas; investigating ML offenses related to smuggling, as well as other criminal investigations. | 2021: 23,056,639 2022: 22,569,466 2023: 26,595,965 |

| Agency Name | Tasks and Duties Related to AML/CFT/CPF | Total Budget (Unit: NTD1,000) |
|---|--|---|
| Ministry of Finance | The Ministry of Finance leads national fiscal administration and is responsible for treasury and payment operations, taxation, customs, national property management, fiscal information, promoting private sector involvement in public infrastructure, and overseeing its subordinate personnel training institutes. The Department of International Fiscal Affairs, under the Ministry, is responsible for negotiating tax treaties with foreign tax authorities and executing cross-border tax information exchange. | 2021: 17,556,213 2022: 17,368,168 2023: 19,339,736 |
| National Taxation Bureau, Ministry of Finance | Responsible for drafting and revising tax laws and regulations; planning, directing, supervising, and evaluating national tax collection operations; overseeing local tax collection efforts; supervising the oversight activities of regional National Taxation Bureaus; auditing and referring major tax evasion cases; and serving as the competent authority for Certified Public Bookkeepers and for Bookkeeping and Tax Return Filing Agent. | 2021: 14,793,123 2022: 14,427,509 2023: 14,646,547 |
| Customs Administration, Ministry of Finance | The four subordinate customs offices—Keelung, Taipei, Taichung, and Kaohsiung—are responsible for administering the declaration and reporting system for travelers and crew members who carry, as well as for those who transport by cargo, express delivery, postal services, or other similar means, large amounts of cash, bearer negotiable instruments, gold, and other items that may be used for money laundering when entering or leaving the country. They are also responsible for international customs cooperation, including assisting with border drug and smuggling cases. | 2021: 6,037,369 2022: 6,582,985 2023: 6,905,740 |
| Financial Supervisory Commission | The Financial Supervisory Commission serves as the supervisory authority for AML/CFT matters within Taiwan's financial markets and financial service industries. These financial markets encompass the banking, bills, securities, futures, financial derivatives markets, and insurance market, along with their respective clearing and settlement systems. The financial service industries include financial holding companies, the Financial Restructuring Fund, the Central Deposit Insurance Corporation, banking, securities, futures, insurance, electronic financial transactions, and other financial service providers. The relevant departments—Banking Bureau, Securities and Futures Bureau, Insurance Bureau, and Examination Bureau—are each responsible for oversight of the development and supervision, management, and inspection of the above financial markets and services under their jurisdiction. Additionally, the Securities and Futures Bureau is responsible for AML measures relating to certified public accountants. | 2021: Banking Bureau: 352,750 Securities and Futures Bureau: 351,705 Insurance Bureau: 162,024 Examination Bureau: 457,266 2022: Banking Bureau: 355,639 Securities and Futures Bureau: 355,809 Insurance Bureau: 167,554 Examination Bureau: 461,576 2023: Banking Bureau: 365,290 Securities and Futures Bureau: 360,705 Insurance Bureau: |

| Agency Name | Tasks and Duties Related to AML/CFT/CPF | Total Budget (Unit: NTD1,000) |
|--|--|---|
| | | 176,428 Examination Bureau: 487,816 |
| Agricultural Finance Agency, Ministry of Agriculture | The supervisory authority for agricultural financial institutions, including the Agricultural Bank of Taiwan and the Credit Departments of Farmers' and Fishermen's Association. | 2021: 150,879 2022: 145,608 2023: 549,696 |
| Central Bank | The Central Bank is the monetary authority of Taiwan, responsible for issuing currency, formulating monetary policy, and managing foreign exchange reserves. In addition, the Central Bank is responsible for managing foreign exchange operations and serves as the supervisory authority for foreign currency exchange dealers. | 2021: 2,103,710 (Operating expenses) 2022: 2,146,002 (Operating expenses) 2023: 2,227,541 (Operating expenses) |
| Ministry of the Interior | Responsible for nationwide internal administrative affairs, its subordinate agencies—including the National Police Agency and the Immigration Agency—investigate predicate crimes and ML and FT offenses. In supervisory matters, it oversees the real estate brokerage industry and land administration agents; manages the establishment, amendment, and interpretation of regulations under the Real Estate Brokerage Management Act; and undertakes the management and guidance of the real estate brokerage industry and brokers, as well as the regulation, certification issuance, business license registration, and oversight of land administration agents. Additionally, the Department of Cooperation and Civil Organizations and the Department of Religious and Ritual Affairs under its jurisdiction supervise the establishment, operation, business guidance, and management of related non-profit organizations. | 2021: 4,047,129 2022: 3,843,827 2023: 14,243,013 |
| Department of Cooperation and Civil Organizations, Ministry of the Interior | Planning, guidance, supervision, and resource empowerment for social organizations, professional groups, and cooperative enterprise policies and systems. | 2021: 32,621 2022: 38,259 2023: 41,223 |
| Department of Religious and Ritual Affairs, Ministry of the Interior ³³ | Planning, promotion, and guidance of policies and systems related to religion, ritual industries, deity associations, funeral management, national emblems and flags, honors and awards, and commemorative days and festivals. | 2021: 955,250 2022: 838,848 2023: 11,105,227 |

³³ The Department of Religious and Ritual Affairs was separated from the Department of Civil Affairs, Ministry of the Interior, on September 20, 2023. Therefore, no separate budget existed for this department from 2021 to 2023; instead, the statutory budgets for the Department of Civil Affairs during those years are provided.

| Agency Name | Tasks and Duties Related to AML/CFT/CPF | Total Budget (Unit: NTD1,000) |
|--|---|---|
| Administration of Commerce, Ministry of Economic Affairs ³⁴ | Responsible for drafting Taiwan's commercial policies and regulations, planning, managing, supervising, and coordinating commercial affairs. This includes registration management and supervision of companies and commercial entities, establishing and revising standards for the classification of commercial groups, and serving as the competent authority for AML and CFT efforts in the jewelry business. | 2021: 18,666,960 (Ministry of Economic Affairs) 2022: 19,714,649 (Ministry of Economic Affairs) 2023: 2,001,981 |
| Administration for Digital Industries, Ministry of Digital Affairs ³⁵ | Serves as the supervisory authority for enterprises or personnel providing third-party payment services and online gaming businesses in Taiwan. | 2023: 2,579,641 |
| Ministry of Foreign Affairs | Responsible for Taiwan's foreign affairs and related international matters. | 2021: 27,871,211 2022: 28,893,770 2023: 30,109,667 |
| Mainland Affairs Council | Responsible for managing exchanges and affairs between Taiwan and Mainland China, Hong Kong, and Macau. | 2021: 938,348 2022: 914,211 2023: 904,414 |
| National Security Office, Executive Yuan | Coordinates and integrates government agencies' efforts in prevention and response to terrorist attacks and major man-made security incidents; promotes protection of critical infrastructure to ensure operational continuity. | 2021: 4,509 2022: 4,323 2023: 4,295 |
| National Security Bureau | Manages international intelligence, intelligence related to Mainland China, and Taiwan regional security intelligence; provides integration, guidance, coordination, and support for national intelligence operations within the Coast Guard Administration, National Police Agency, Immigration Agency, and the Investigation Bureau of the Ministry of Justice. It is also responsible for collecting and disseminating intelligence related to FT. | Confidential |
| International Trade Administration, Ministry of Economic Affairs | Responsible for formulating Taiwan's international trade policies, trade promotion, import and export management, and export control of strategic high-tech commodities. | 2021: 1,631,084 2022: 1,695,658 2023: 1,586,880 |
| Ministry of Health and Welfare | Responsible for Taiwan's healthcare and social welfare policies; supervises medical foundations and social welfare foundations. | 2021: 204,868,474 2022: 203,037,592 2023: 223,096,819 |
| Ministry of Education | Responsible for education policies in Taiwan and serves as the competent authority for educational foundations. Regulatory categories encompass school foundations at various levels, including universities and colleges, as well as senior high schools, vocational schools (private schools), and foundations engaged in education, youth development, and sports affairs. | 2021: 132,153,090 2022: 136,547,706 2023: 138,871,365 |

³⁴ The Administration of Commerce was reorganized into the Department of Commerce Development on September 26, 2023. Since its 2021 and 2022 budgets were included within the Ministry of Economic Affairs, they cannot be separately detailed. Therefore, the statutory budgets of the Ministry of Economic Affairs for 2021 and 2022 are provided.

³⁵ Administration for Digital Industries was established on August 27, 2022, so statutory budget data are available only for 2023.

| Agency Name | Tasks and Duties Related to AML/CFT/CPF | Total Budget (Unit: NTD1,000) |
|---------------------|---|--|
| Ministry of Culture | The Ministry is responsible for supervising cultural foundations (including those established with government or private donations) as well as the visual arts industry. Its main missions are to promote the development of the cultural and artistic environment, support cultural and artistic activities, and strengthen the health of the industry market. | 2021: 11,447,397 2022: 11,102,172 2023: 12,770,226 |

Department of Religious and Ritual Affairs, Administration of Commerce, Ministry of Economic Affairs³⁴; Administration for Digital Industries, Ministry of Digital Affairs³⁵

Annex 3: Factors and Classification Definitions for Money Laundering Threat Analysis

| Definitions of Rating Factors for Money Laundering Threats | | | | | |
|--|--|---|--|--|--|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| Criminal Capability | The criminal demonstrates knowledge, skills, expertise, networks, and resources related to ML, especially in areas such as finance, trade, law, IT, and awareness of AML controls, using these to evade supervisory authority detection. | The criminal shows complexity, has well-established networks, and possesses substantial resources to support complex, long-term, and large-scale ML activities. | The criminal demonstrates moderate complexity and has significant resources for conducting long-term or non-permanent ML actions. | The criminal exhibits some complexity and possesses limited resources to conduct simple ML activities. | The criminal's capability to engage in complex ML activities is minimal; their ML actions are restricted to immediate handling or integration of illicit proceeds for personal use. The criminal largely relies on their personal resources and has no existing network. |
| Scope of Money Laundering Activities | This item measures the extent to which criminals use financial institutions, DNFBPs, and other sectors to launder criminal proceeds. | The criminal exploits multiple domestic and overseas sectors to maintain high capability for allocating funds and illicit proceeds abroad. | The criminal exploits a limited number of domestic or international sectors to maintain considerable capability to allocate funds and illicit proceeds abroad. | The criminal exploits a limited number of domestic sectors, with limited capability to allocate funds and illicit proceeds abroad (e.g., sectors of limited size, offering limited product or partnerships). | The criminal exploits a single domestic sector. |

| Definitions of Rating Factors for Money Laundering Threats | | | | | |
|--|---|----------------------|-----------------------------|-------------------------|--------------------------|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| Estimated value of criminal proceeds (NTD) | Illegal proceeds generated from a single predicate offense or professional ML | NTD1 billion or more | Hundreds of millions of NTD | Tens of millions of NTD | Millions of NTD or below |

Annex 4: Factors and Classification Definitions for Terrorist Financing Threat Analysis

| Definitions of Rating Factors for Terrorist Financing Threats | | | | | |
|---|---|---|---|---|---|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| Capability of Terrorist Financiers: 1. Degree of direct/indirect contact with terrorist organizations 2. Knowledge, skills, and expertise in conducting terrorist financing 3. Network, resources, and capacity to carry out terrorist financing activities | The complexity, networks, and resources of terrorist financiers enable them to quickly recover, sustain, and carry out long-term terrorist financing activities. Key considerations include the organizational structure, size, complexity of the terrorist group, and various fundraising methods. | Terrorist financiers have extensive and robust capabilities to support complex, long-term, and large-scale terrorist financing activities within the country. | Terrorist financiers have sufficient capabilities to support significant terrorist financing activities in the country. | Terrorist financiers have some capabilities to conduct simple terrorist financing activities in the country. | Terrorist financiers have minimal capabilities, and terrorist financing activities are sporadic and negligible. |
| Global Scope of Activities: 1. Extent and geographical range of terrorist financing operations 2. Diversity of sources and methods for terrorist financiers to | Terrorist financiers have a network of supporters and sympathizers who can quickly mobilize to facilitate terrorist activities. | The network of supporters for terrorist financiers spans the globe, with supporters located in multiple countries or regions. | The network of supporters for terrorist financiers exists in only a few countries or regions worldwide. | The network of supporters for terrorist financiers is predominantly overseas, but there are some supporters domestically. | The network of supporters for terrorist financiers is mostly overseas, and the number of supporters within the local community is negligible. |

| Definitions of Rating Factors for Terrorist Financing Threats | | | | | |
|---|--|-----------------------|-------------------------------|----------------------------|------------------|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| collect and handle funds 3. Degree to which raised funds are used to harm national or international interests. | | | | | |
| Estimated funds that can be raised annually in the country (NTD): 1. Estimated annual terrorist financing amount | This estimate should consider all types of support, including financial and material support, and encompass both legitimate funds and proceeds of crime. | NTD10 million or more | NTD1 million to NTD10 million | NTD100,000 to NTD1 million | below NTD100,000 |

Annex 5: Factors and Classification Definitions for Money Laundering and Terrorist Financing Vulnerability Analysis

| Definition of Sectoral Vulnerability Assessment Factors | | | | | |
|---|--|---|--|---|---|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| Inherent Characteristics of the Sector | <p>This rating should consider the sector's importance in the domestic economy, as well as whether its structure and operating locations facilitate the rapid movement of funds. The following should be considered collectively:</p> <ul style="list-style-type: none"> ● Sector size: total transaction volume and total assets of the sector ● Complexity of the sector's business structure ● Degree of integration with other reporting sectors ● Business operation locations: This criterion refers to the extent to which customers have access to the industry's products and services. | <p>This industry is considered to have both high transaction volumes and large asset sizes.</p> <p>The industry structure is complex and is well-integrated with other sectors.</p> <p>Its business locations are prevalent both domestically and internationally.</p> <p>Given the above, the industry can be widely used by many customers and offers significant</p> | <p>This industry is considered to have average transaction volumes and asset size.</p> <p>Its structure contains certain complex factors, allowing a certain degree of integration with other industries.</p> <p>Its business locations are prevalent domestically.</p> <p>Given the above, the industry can be used by most customers and provides a moderate</p> | <p>This industry is considered to be small in both transaction volume and asset size.</p> <p>Its structure is less complex, with limited integration with other sectors.</p> <p>Business locations are limited.</p> <p>Given the above, the industry can be used by a few customers and provides limited fund</p> | <p>The sector involves occasional activities with only a small number of transactions.</p> <p>Its structure is simple and is rarely integrated with other sectors.</p> <p>Business locations are limited.</p> <p>Given the above, the industry is only used by a single customer under specific circum-</p> |

| Definition of Sectoral Vulnerability Assessment Factors | | | | | |
|---|--|--|---|--|---|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| | | fund transfer capabilities. | level of fund transfer capability. | transfer capability. | tances, and there is virtually no ability to transfer funds within or outside the industry. |
| Nature of Products and Services Offered by the Industry | <p>The nature of products and services carries varying degrees of inherent vulnerabilities. Accordingly, when determining the rating for this factor, the following considerations will be made:</p> <ul style="list-style-type: none"> ● The nature and scope of the products and services offered: This standard focuses on products and services commonly identified as vulnerable to money laundering and terrorist financing, including the following: <ul style="list-style-type: none"> ➢ Products and services that involve the possibility of cash payments and monetary instruments ➢ Private banking ➢ Trade finance services, such as export letters of credit ➢ Products and services utilizing emerging technologies | <p>The sector offers a large number of vulnerable (easily exploited) products and services.</p> <p>These constitute a significant portion of the sector's overall business operations.</p> <p>The transaction volume and frequency associated with these specific products are considered high.</p> <p>Such transactions can be found in numerous investigative cases.</p> | <p>The sector offers a limited number of vulnerable (easily exploited) products and services.</p> <p>These constitute a vital component of the sector's overall business operations.</p> <p>The transaction volume and frequency associated with these specific products are considered significant.</p> <p>Such transactions can be found in some investigative cases.</p> | <p>The sector offers only a single or a minimal range of products and services.</p> <p>These constitute only a small part of the sector's overall business/operations.</p> <p>The transaction volume and frequency associated with these specific products are considered moderate.</p> <p>Such transactions can be found in only a small number of investigative cases.</p> | <p>The products and services of the sector are limited to non-deposit activities involving small cash transactions only.</p> <p>The amounts involved in such transactions are relatively low.</p> <p>The products and services provided are also subject to the restricted use of funds.</p> <p>There are no investigative cases involving such transactions.</p> |

| Definition of Sectoral Vulnerability Assessment Factors | | | | | |
|---|---|---|---|---|--|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| | <ul style="list-style-type: none"> ➤ Services or products capable of cross-border funds transfer, including electronic funds transfer ➤ High-value goods (such as gold, precious metals, gemstones, automobiles, and works of art) ➤ Other goods and services identified during investigations | | | | |
| Nature of business relationship with customers | <p>This assessment factor seeks to identify inherent vulnerabilities related to customer data in the sector. The following elements are taken into account:</p> <ul style="list-style-type: none"> ● Nature of business relationship: This criterion determines whether most customers are engaged in ongoing relationships or transactional relationships and whether relationships are direct or indirect. ● Customer identity: To assess this criterion, consider the significance of foreign, domestic, or international PEPs within the customer data of the sector. ● Customer occupation/business activity: Certain customer activities are recognized as | The sector's customer composition demonstrates a combination of most vulnerability factors, including transactional and/or indirect business relationships, PEPs, and customers engaged in occupations/business with increased vulnerability. | The sector's customer composition reveals a combination of vulnerabilities, including transactional relationships and/or third-party business relationships; PEPs; and customers engaged in inherently vulnerable occupations/business. | The sector's clientele includes limited interaction with customers involved in transactional relationships and/or third-party business relationships; PEPs; and customers engaged in occupations/business prone to vulnerabilities. | The customers of the industry do not include or include very limited number of clients who are vulnerable to risks. Where customers are vulnerable to ML/FT, operations are only occasional and limited. |

| Definition of Sectoral Vulnerability Assessment Factors | | | | | |
|---|--|---|--|--|--|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| | inherently more vulnerable to money laundering/terrorist financing (ML/FT). When evaluating the sector's customer base, the following factors will be considered: the proportion of high-net-worth individuals, the presence of cash-intensive businesses, and the degree to which the beneficial ownership of most customers is easily identifiable (e.g., complexity of business structures or individual profiles). | | | | |
| Geographical scope of industry activities | <p>In considering the degree of vulnerability associated with this factor, the following aspects involved in an industry's activities are evaluated:</p> <ul style="list-style-type: none"> ● High-risk jurisdictions: jurisdictions identified by the Financial Action Task Force (FATF) or regional FATF-style bodies as high-risk. ● Jurisdictions of concern for ML and FT that, while not designated as high-risk by the FATF, exhibit significant informal banking | The sector's activities involve high-risk jurisdictions or countries with significant informal banking sectors, which are jurisdictions of concern. Activities in these locations comprise significant business operations for the sector and are | The sector's activities involve high-risk jurisdictions or countries with significant informal banking sectors, which are jurisdictions of concern. Activities in these locations do not comprise significant business operations for the sector | The sector's activities may involve high-risk jurisdictions, important informal banking sectors, or jurisdictions of concern. However, the level of business conducted in these locations is relatively minor in the sector's overall activity and is not continual or | The sector's activities are restricted to domestic operations and do not involve locations of concern. |

| Definition of Sectoral Vulnerability Assessment Factors | | | | | |
|---|--|---|--|---|---|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| | <p>sectors, corruption (as indicated by World Bank and Transparency International data); considerable social, economic, and institutional instability; banking secrecy, or are recognized as tax havens or vulnerable to abuse.</p> <ul style="list-style-type: none"> ● Jurisdictions or locations of national security concern | conducted on a continual and regular basis. | but are conducted on a continual and regular basis. | regular. | |
| Nature of service channels | <p>The following aspects are considered when assessing the weakness level related to this factor:</p> <ul style="list-style-type: none"> ● Anonymity afforded by the service channels used (e.g., both parties face-to-face; both parties and agent/third party face-to-face; both parties non-face-to-face; non-face-to-face with agents or third parties) ● Their complexity (e.g., multiple intermediaries with only a few under direct control and little or no responsibility to identify the originator of the transaction). | Most transactions within the sector are conducted through service channels involving high anonymity and complexity. | Most transactions within the sector are conducted through service channels with high anonymity and complexity. | Transactions are occasionally conducted through service channels involving high anonymity and complexity (not constituting primary service channels). | No or rare complex and anonymous service channels |

Annex 6: Factors and Classification Definitions for Proliferation Financing Threat Analysis

| Definitions of Proliferation Financing Threat Rating Factors | | | | | |
|--|--|---|---|---|--|
| Selected Rating Factors | Definition | Very High | High | Moderate | Low |
| Actor Capability | The actor possesses criminal knowledge, skills, expertise, networks, and resources, particularly in finance, trade, law, information technology, and awareness of counter-proliferation and control measures and applies this knowledge to evade detection by supervisory authorities. | The actor exhibits widespread complexity, has established robust networks, and possesses substantial resources to support complex, long-term, and large-scale proliferation financing operations. | The actor has considerable complexity and possesses significant resources to carry out long-term or non-long-term proliferation financing activities. | The actor has some complexity and limited resources to engage in simple proliferation financing activities. | The actor's capability to conduct proliferation financing is minimal, mainly relying on personal resources with no existing network. |
| Scope of Proliferation Financing Activities | This measures the extent to which the actor uses financial institutions, DNFBPs, and other industries to finance proliferation. | The actor leverages multiple domestic and foreign sectors to maintain high capability to achieve proliferation financing objectives. | The actor uses a limited number of domestic or international sectors to maintain considerable capability to achieve proliferation financing goals. | The actor uses a limited number of domestic sectors with limited capability (e.g., operators of limited scale or those providing limited products or partners). | The actor operates through a single domestic sector. |
| Estimated Criminal Proceeds | Value of illicit proceeds generated by proliferation financing activities | NTD1 billion or more | Hundreds of millions of NTD | Tens of millions of NTD | millions of NTD or below |

Annex 7: Factors and Classification Definitions for Proliferation Financing Vulnerability Analysis

| Definition of Proliferation Financing Vulnerability Rating Factors | | | | |
|--|--|---|--|--|
| Selected Rating Factors | Definition | High | Moderate | Low |
| Geographical Environment Factors | Relationship with the country's geographical and environmental background. | The country's geographical environment is highly conducive to actors engaging in proliferation financing activities. | The country's geographical environment background only partly favors actors engaging in proliferation financing activities in certain areas or conditions. | The country's geographical environment is unfavorable to actors engaging in proliferation financing activities. |
| Political and Social Factors | The country's political will to combat proliferation, proliferation financing, and social factors. | The country lacks the political will to combat proliferation financing and has related social factors influencing this. | The country has the political will to combat proliferation financing but is affected by related social factors. | The country has a strong political will to combat proliferation financing and is not affected by related social factors. |
| Laws and Institutional Factors | <ol style="list-style-type: none"> 1. Law enforcement's capacity to combat proliferation financing 2. Current state of international cooperation (including difficulties) 3. Legislation and related measures enacted by the country to counter proliferation financing, the implementation status of United Nations Security Council resolutions on targeted | <p>The legal framework/regulatory mechanism has significant gaps or major omissions, and communication between the public and private sectors is weak; in practice (law enforcement /supervision), a large number of cases cannot be investigated or are difficult to investigate or prosecute. (May include the following situations: Possible</p> | <p>Legal framework/regulatory mechanism is generally regulated, and public-private sector communication and interaction are conducted regularly; practical implementation (law enforcement /supervision) difficulties can be resolved through existing mechanisms, with no significant (insurmountable) obstacles.</p> | <p>Legal framework/regulatory mechanisms are regulated, with close communication and interaction between public and private sectors; no obstructive issues in practical implementation (law enforcement/supervision) (May include the following situations: 1. Related laws and institutions</p> |

| Definition of Proliferation Financing Vulnerability Rating Factors | | | | |
|--|---|---|---|---|
| Selected Rating Factors | Definition | High | Moderate | Low |
| | <p>financial sanctions related to proliferation financing, and compliance with FATF standards, especially Recommendation 7 and Immediate Outcome 11.</p> <p>4. National implementation status of United Nations sanctions, embargoes, or other measures.</p> <p>5. National export control and/or regulatory mechanism implementation status.</p> <p>6. Public and private sector advocacy, guidance, or awareness-raising actions related to combating proliferation financing, including the sharing of proliferation financing red flags and typologies.</p> <p>7. Shipping registration status, including record keeping of the flag of convenience</p> | <p>1. related legal and institutional significant gaps, limited implementation, and capacity.</p> <p>2. Limited international cooperation implementation and inability to obtain adequate responses</p> <p>3. Law enforcement agencies have limited investigation capabilities for proliferation financing cases, face difficulties in evidence collection, and rely heavily on international intelligence.</p> <p>4. Inability to obtain relevant evidence and lacking sufficient capacity to investigate cyberattack incidents by sanctioned countries.</p> <p>5. Relevant departments face</p> | <p>(May include the following situations:</p> <p>1. Related laws and institutions have few gaps; implementation and capacity are adequate.</p> <p>2. International cooperation implementation is adequate; appropriate responses can be obtained.</p> <p>3. Law enforcement agencies have adequate investigation capabilities for proliferation financing cases and can collect evidence, relying on international intelligence only in some cases.</p> <p>4. Partial evidence and ability to investigate cyberattack incidents by sanctioned countries.</p> <p>5. Some difficulties persist among relevant</p> | <p>are comprehensive; implementation and capacity are exemplary.</p> <p>2. International cooperation implementation is exemplary, with appropriate and timely responses available.</p> <p>3. Law enforcement agencies have good investigation capabilities for proliferation financing cases, are capable of initiating investigations and collecting evidence independently, and rely on international intelligence only in a few instances.</p> <p>4. Capable of obtaining relevant evidence and investigating cyberattack incidents originating from sanctioned countries.</p> |

| Definition of Proliferation Financing Vulnerability Rating Factors | | | | |
|--|--|---|--|---|
| Selected Rating Factors | Definition | High | Moderate | Low |
| | | <p>difficulties in implementing targeted financial sanctions, and insufficient horizontal communication results in delayed or incomplete enforcement of targeted economic sanctions.</p> <p>6. Industries have not implemented relevant counter-proliferation measures and are unable to identify evasion of proliferation sanctions.</p> <p>7. Loose regulation in industries, weak related promotion, and awareness.)</p> | <p>departments in implementing targeted financial sanctions despite some horizontal communication. Although targeted sanctions can be implemented, they have not yet been fully realized.</p> <p>6. Some industries have partially implemented relevant counter-proliferation measures and can identify some evasion of proliferation sanctions.</p> <p>7. Slight deficiencies in industry regulation, moderate related promotion, and awareness.)</p> | <p>5. Relevant departments can swiftly implement targeted financial sanctions, communicate effectively, and fully execute them.</p> <p>6. Industries have implemented relevant counter-proliferation measures sufficient to identify evasion of proliferation sanctions.</p> <p>7. Sound industry regulation, sufficient related promotion, and awareness.)</p> |
| Economic and technical factors | 1. Current status includes establishment details (registrable entities, quantity, scale, etc.) and regulatory framework, | Relevant industries account for a significant share of the domestic economy but exhibit weak compliance awareness; | Relevant industries occupy a specific economic scale domestically; although compliance awareness exists, illegal | Relevant industries account for a very low proportion of the domestic economic scale, with high compliance |

| Definition of Proliferation Financing Vulnerability Rating Factors | | | | |
|--|--|---|--|--|
| Selected Rating Factors | Definition | High | Moderate | Low |
| | <p>as well as the promotion status of the virtual asset industry—covering virtual currency exchanges, OTC platforms, and custodial wallet providers, including those not registered domestically.</p> <p>2. Current status of controls and audit mechanisms related to the trade or transit of funds and goods</p> <p>3. Analysis of dual-use or controlled goods industries and/or trade, high-tech industry, and/or trade</p> <p>4. Current status of international fund transfers and access to global markets</p> <p>5. Current status analysis of the maritime or cargo insurance or reinsurance industry</p> <p>6. Current status analysis of the marine fuel industry</p> <p>7. Current status analysis of the trade finance industry</p> | <p>numerous cases of illegal transactions involving North Korea and Iran are frequently observed in practice. (May include the following situations:</p> <p>1. In many investigation cases, various industries are abused for proliferation financing activities.</p> <p>2. Dual-use industries, marine fuel industries, and frequent trade comprise a significant part of overall trade.</p> <p>3. Financial institutions provide certain related trade finance services to countries subject to proliferation sanctions, accounting for a high proportion of total services.)</p> | <p>transaction cases involving North Korea/Iran continue. (May include the following situations:</p> <p>1. In some investigation cases, various industries are abused for proliferation financing activities.</p> <p>2. Dual-use industries, marine fuel industries, and moderate trade are only part of the overall trade.</p> <p>3. Financial institutions offer a limited range of trade finance services to countries subject to proliferation sanctions, accounting for only a small proportion of their total services.)</p> | <p>awareness and rare illegal transaction cases involving North Korea/Iran. (May include the following situations:</p> <p>1. No cases were found in investigations showing industries abusing their roles for proliferation financing activities.</p> <p>2. Dual-use industries, marine fuel industries, and sparse trade; only a negligible proportion of overall trade.</p> <p>3. Financial institutions provide sporadic related trade finance services to countries subject to proliferation sanctions, accounting for a very low proportion of total services.)</p> |

| Definition of Proliferation Financing Vulnerability Rating Factors | | | | |
|--|---|---|--|--|
| Selected Rating Factors | Definition | High | Moderate | Low |
| Legal persons and Arrangements/Trusts | The status of transparency of legal persons and arrangements/trusts, including the beneficial ownership structure of companies. | <p>Significant gaps in the legal framework/supervisory mechanisms make it challenging to identify the structure and beneficial owners of legal persons and arrangements. (May include the following situations:</p> <ol style="list-style-type: none"> 1. Industries struggle to obtain beneficial ownership information, which is crucial for identifying cases related to the evasion of proliferation sanctions due to limited capacity to confirm the identity of beneficial owners. 2. No relevant legal transparency regulations for legal persons and no related confirmation mechanisms exist.) | <p>Existing legal frameworks and supervisory mechanisms are insufficient, posing difficulties in identifying the structure and beneficial owners of legal persons and arrangements; however, identification may be assisted through other mechanisms (May include the following:</p> <ol style="list-style-type: none"> 1. Industries can still obtain partial beneficial ownership information to identify cases of proliferation sanctions evasion and have some capacity to verify the identities of beneficial owners. 2. Relevant corporate transparency regulations have been enacted, and specific provisions have been implemented.) | <p>The existing legal framework and supervisory mechanisms are complete, enabling the comprehensive and practical identification of the structure and beneficial owners of legal persons and arrangements. (May include the following situations:</p> <ol style="list-style-type: none"> 1. Industries can fully obtain and understand information related to beneficial owners, enabling them to identify and prevent sanctions evasion related to proliferation financing and verify relevant identities. 2. Related corporate transparency regulations have been enacted and adequately implemented.) |

Appendix: Meeting Minutes Compilation

First National ML/TF/PF Risk Assessment Meeting (2024.7.22)



Second National ML/TF/PF Risk Assessment Meeting (2024.7.29)



Third National ML/TF/PF Risk Assessment Meeting (2024.7.30)



Fourth National ML/TF/PF Risk Assessment Meeting (2024.8.30)



Fifth National ML/TF/PF Risk Assessment Meeting (2024.9.6)



Sixth National ML/TF/PF Risk Assessment Meeting (2024.9.12)



