PARALLEL REPORT

On 《ROC's Third Report under the United Nations Convention against Corruption》

Reporting Entity:

Taiwan Anti-Fraud and Forensic Accounting Association

(ACFE, Taiwan Chapter)

I. Introduction

Owing to complex international political realities, Taiwan has thus far been unable to become a Member State of the United Nations. Nonetheless, our country remains actively engaged with the international community and makes every effort to adhere to the global standards established by various United Nations conventions. In 2015, Taiwan enacted the "Act to Implement United Nations Convention against Corruption" (hereinafter referred to as the "UNCAC Implementation Act") as a concrete measure to give effect to the United Nations Convention against Corruption (UNCAC). Pursuant to Article 2 of the Act, the anti-corruption policies, institutional systems, and measures prescribed in the Convention have been granted domestic legal status.

In strict compliance with the periodic national reporting mechanisms mandated by Article 6 of the UNCAC Implementation Act, the Executive Yuan successfully compiled and published the Initial National Report under UNCAC in 2018 and the Second National Report under UNCAC in 2022, respectively. Most recently, in April 2026, the government released "ROC's Third Report under the United Nations Convention against Corruption." By subjecting these periodic reports to rigorous domestic self-assessment and international peer reviews led by globally renowned experts, Taiwan consistently demonstrates its unyielding determination to combat corruption and maintain alignment with global anti-corruption legal frameworks.

Taiwan Anti-fraud and Forensic Accounting Association, serving as the sole official affiliate of the ACFE in Taiwan, is deeply dedicated to developing and promoting professional expertise, standards, and practical methodologies in the fields of anti-fraud, compliance, and forensic accounting investigation. Advancing anti-corruption efforts is a core pillar of our organizational mission. Over the years, the Association has continuously acted as an impartial, public-interest third-party observer, tracking domestic and cross-border corruption incidents and analyzing international law enforcement trends to provide constructive, independent feedback. To build upon the insights of the newly released Third National Report, the Association hereby submits this Parallel Report on "ROC's Third Report under the United Nations Convention against Corruption," aiming to serve as a comprehensive strategic reference for future governmental policymaking, anti-fraud enforcement, and legal system enhancements.

II. Executive Summary

According to the "Occupational Fraud 2026: A Report to the Nations" published globally by the Association of Certified Fraud Examiners (ACFE), corruption and bribery schemes continue to represent an exceptionally severe challenge within organizational misconduct. Globally, the proportion of occupational fraud cases involving corrupt activities has reached a staggering 45%, showing a pronounced, long-term upward trend surging from a mere 10% in 1996 to the current 45% in 2026. This vulnerability is significantly magnified in the Asia-Pacific region, where over 60% of all reported occupational fraud cases are directly intertwined with corrupt schemes. Furthermore, the global median loss caused per individual corruption case stands at a substantial USD 150,000. These metrics highlight that corruption is no longer a localized, isolated issue of individual moral failure or momentary lapse in ethical judgment; rather, it has evolved into a deeply rooted, systemic governance risk that demands aggressive, synchronized public-private partnerships and institutional controls.

Grounded in a decade of rigorous practical investigations, legislative advocacy, and academic insights accumulated since our founding, the Association has comprehensively reviewed the self-assessment disclosures in Taiwan's Third National Report, alongside the implementation status of the 30 Concluding Observations delivered during the Second International Review. To guide future reforms, the Association presents ten core findings and recommendations as below:

1. **Expeditiously Complete Legislation for Private Sector Bribery**
   Amendments to criminalize private sector bribery have encountered persistent delays. The government must treat commercial bribery as a top-priority standalone offense, moving beyond traditional breach of trust constraints to protect market fairness and competitive environments.

2. **Eliminate Public-Private Separations in Whistleblower Protection Laws**
   The current public-private separations in whistleblower frameworks weakens compliance structures. In alignment with UNCAC Article 33, standard protection measures, job security, and identity confidentiality must be expanded systematically to encompass private sector reporting person.

3. **Promote the Establishment of Corporate Anti-Corruption Committees**

   Anti-corruption mechanisms within private enterprises remain functionally weak. The state should leverage public-private partnership models to guide and incentivize legal entities across key industries to establish independent, expert-led internal Anti-Corruption Committees.

4. **Structure a Comprehensive Framework for Corporate Criminal Liability**

   Taiwan lacks direct criminal liability for legal persons involved in systemic corruption, relying primarily on natural-person sanctions. A robust, standalone corporate criminal liability framework—incorporating proactive compliance mechanisms as affirmative defenses—must be accelerated.

5. **Establish a Comprehensive Reporting and Disclosure System for Beneficial Ownership Information**

   Current thresholds fail to sufficiently identify natural persons with ultimate substantial control over legal entities. Taiwan must establish a centralized registry for beneficial ownership matching FATF international standards to narrow the space for opaque corporate vehicles and criminal cash flows.

6. **Improve Judicial Transparency by Disclosing Forensic Accounting and Appraisal Reports in Full**
   Access to critical expert evidence in trials remains heavily restricted. To strengthen public oversight and safeguard systemic accountability, the full text of forensic accounting reports and judicial appraisal reports utilized in public-interest litigations must be proactively disclosed.

7. **Utilize Automation and AI Technologies to Enhance the Capabilities of Corruption Prevention and Investigation**
   In response to emerging data complexities, manual auditing must be augmented. Government supervisory bodies should incorporate robotic process automation (RPA), predictive machine learning, and AI alert mechanisms to systematically evaluate agency risks and flag high-risk public procurements early.

8. **Accelerate the Statutory Authorization for Special Compulsory Investigative Measures**
   Law enforcement agencies face operational gridlock due to slow legislative processes regarding technology-driven evidence collection. The Science and Technology Investigation Act and related compulsory measures must be completed to grant clear, legally sound authorization for surveillance and digital forensics.

9. Enact the Virtual Asset Supervision Act and Enforce the Travel Rule

The decentralized, anonymous nature of digital assets has created significant regulatory blind spots used by money laundering rings. Taiwan must rapidly move past loose guidelines to institute a binding supervision act for virtual assets, mandating full implementation of the FATF Travel Rule.

10. Formally Include the "Certified Fraud Examiner(CFE)" Credential in the Qualification Requirements for Internal Auditors

To deepen international technical exchange and enhance organizational governance, the Financial Supervisory Commission (FSC) should formally include the globally recognized Certified Fraud Examiner (CFE) credential as a valid and preferred criteria for certifying qualified internal auditors.

To ensure structured monitoring and programmatic implementation, the Association's ten core findings and recommendations are systematically mapped against the specific provisions of the United Nations Convention against Corruption (UNCAC) and the corresponding Concluding Observations from the Second International Review below:

No.	Association's Core Findings & Recommendations	Corresponding UNCAC Articles	Corresponding Concluding Observations (Second International Review)
1.	Delay in criminalizing private sector bribery; complete commercial bribery legislation as soon as possible.	Article 12 (Private sector) Article 21 (Bribery in the private sector) Article 35 (Compensation for damage)	Recommendation No. 15: Criminalize bribery in the private sector. Recommendation No. 22: Revise the definition of victim of corruption.
2.	Public-private separation violates the spirit of the Convention; expand whistleblower protection to include the private sector.	Article 33 (Protection of reporting persons)	Recommendation No. 5: Establish anonymous whistleblowing channels for both public and private sectors. Recommendation No. 21: Promote the Whistleblower Protection Act.

3.	Weak private sector anti-corruption mechanisms; promote the establishment of anti-corruption committees.	Article 12 (Private sector) Article 21 (Bribery in the private sector)	Recommendation No. 11: Promote anti-corruption efforts in the private sector through public-private partnerships.
4.	Lack of corporate liability for corruption; build a comprehensive corporate criminal liability system.	Article 26 (Liability of legal persons)	Recommendation No. 17: Establish legal liability for corporate corruption.
5.	Insufficient disclosure of beneficial ownership information; establish a comprehensive reporting and disclosure system.	Article 9 (Public procurement and management of public finances) Article 12 (Private sector) Article 52 (Prevention and detection of transfers of proceeds of crime)	Recommendation No. 7: Disclose the beneficial owners of government procurements. Recommendation No. 10: Establish a centralized registration system for beneficial ownership. Recommendation No. 27: Identify individuals who are the actual controllers of

			companies and flexibly disclose the information registered by beneficial owners.
6.	Insufficient court transparency; promote full public disclosure of forensic accounting and appraisal reports.	Article 10 (Public reporting) Article 11 (Measures relating to the judiciary and prosecution services) Article 32 (Protection of witnesses, experts and victims)	Recommendation No. 9: Establish a dedicated agency to handle complaints regarding compliance with the Freedom of Government Information Law.
7.	In response to AI technology development, utilize automation and AI to enhance prevention and investigation capabilities.	Article 5 (Preventive anti-corruption policies and practices) Article 50 (Special investigative techniques)	Recommendation No. 8: Establish a systematic approach to risk assessment for government agencies.

8.	Slow progress in amending special compulsory measures; accelerate legislation to support investigation practices.	Article 50 (Special investigative techniques)	Recommendation No. 24: Complete the legislation of the undercover and technological investigation laws.
9.	Omissions in current virtual asset control measures; formulate a dedicated virtual asset supervision act and implement the Travel Rule.	Article 14 (Measures to prevent money-laundering) Article 52 (Prevention and detection of transfers of proceeds of crime)	Recommendation No. 12: Strengthen cooperation among anti-money laundering investigation agencies. Recommendation No. 28: Strengthen asset recovery and disposal.
10.	Deepen international anti-corruption technical exchanges; include the Certified Fraud Examiner (CFE) credential in the qualifications for internal auditors.	Article 60 (Training and technical assistance)	Recommendation No. 29: Providing technical assistance through international experience sharing.

III. Findings and Recommendations

1. Expeditiously Complete Legislation for Private Sector Bribery

1.1 Observations and Findings

1.1.1 Core Loophole in Taiwan's Anti-Corruption Legal Framework: Breach of Trust Provisions Struggle to Effectively Prosecute Private Sector Corruption

Commercial bribery in the private sector is an economic crime that erodes fair competition in the free market and compromises shareholder rights and interests. While an international consensus on criminalizing commercial bribery has long been established, Taiwan's legislative progress remains stymied by an ongoing policy debate over whether to focus on "protecting private sector property interests" versus "safeguarding abstract social interests in fair competition." Taiwan's current legal framework relies primarily on the offense of general breach of trust under the Criminal Code to address private sector commercial bribery. In judicial practice, prosecutors are required to prove that the conduct caused actual, quantifiable, and substantial pecuniary loss to the company. Commercial bribery, however, often causes lost profits or opportunity losses, or actual losses that are difficult to quantify. Consequently, this may result in non-prosecution decisions or acquittals, creating a major legal loophole in enforcement practice.

1.1.2 Legal Definition and Remedies for Victims of Corruption

Under the current legal framework, "victims of corruption" and their corresponding relief procedures are not explicitly defined by statute. Instead, relief operates through an integrated framework encompassing class action lawsuits under the Code of Civil Procedure, civil actions incidental to criminal proceedings under the Code of Criminal Procedure, and claims under the State Compensation Law. In judicial practice, however, only the Securities and Futures Investors Protection Center (SFIPC) under the Securities and Exchange Act actively pursues civil compensation for the investing public facing collective damages in securities or futures markets through class actions and representative lawsuits, thereby securing compensation for investors' property losses. Conversely, in other private sector corruption proceedings, however, the procedural status and standing of collective or indirect victims remain inadequately recognized, and clear statutory definitions and remedies are lacking.

1.2 Recommendations

Enact a "Special Breach of Trust" Offense for Commercial Bribery

The legislature should model after the statutory structure of "Special Breach of Trust" under the Banking Act by amending the Criminal Code to establish a standalone "Special Breach of Trust" offense targeting private sector commercial bribery and kickback schemes as an independent criminal offense. Crucially, the legislative scope of damages under breach of trust should be expanded to explicitly incorporate "lost profits and indirect economic losses", such as losses arising from impaired fair competition, the loss of better contracting or bargaining opportunities, material shortages, or increased foreign-exchange risk, should be expressly included within the protected property interests. This would thoroughly resolve the evidentiary hurdles and legal loopholes associated with general breach of trust in commercial bribery cases, overcome the dilemma of prosecuting private sector bribery, and fulfill the spirit of the Convention regarding the inclusion of indirect and collective damages in the definition of victims.

Furthermore, regarding damage calculation methodologies in corruption offenses, the roles of appraisers and expert witnesses should be enhanced through the integration of "quantitative forensic methodologies" from forensic accounting as a technical supporting mechanism. Financial and accounting models can convert lost profits and opportunity losses into monetary measures and provide judges and prosecutors with a concrete basis for quantifying indirect losses, thereby assisting in resolving complex judicial disputes.

2. Eliminate Public-Private Separations in Whistleblower Protection Laws

2.1 Observations and Findings

2.1.1 Legislative Public-Private Separation Leaves the Private Sector in a Protection Vacuum

The Public Interest Whistleblower Protection Act, which came into force in Taiwan in July 2025, established statutory safeguards for whistleblowers within the "pan-public sector", including government agencies, state-owned enterprises, and government-controlled foundations. These protections encompass job security, identity confidentiality, personal safety protection, prohibition of adverse actions (anti-retaliation provisions), and a reversed burden of proof.

However, during the legislative process, the government adopted a passive "public-private separation" strategy under the rationale of "minimizing impact." The final enacted law completely excluded private sector whistleblowers from its statutory protective umbrella. Instead, the government has relied on nonbinding measures, including projects approved by the Executive Yuan, administrative guidance, revisions to model government-procurement contracts, and encouragement for listed companies to incorporate whistleblower protection into their ethical corporate management codes. These measures lack mandatory legal force and fail to satisfy international standards and the recommendations of international review committee members who called for comprehensive, unified legislation covering both the public and private sectors.

2.1.2 Lack of Statutory Protection Exposes Whistleblowers to High Career and Personal Risks

According to the Occupational Fraud 2026: A Report to the Nations published by the Association of Certified Fraud Examiners (ACFE), internal employee "tips" remain the single most effective means of preventing organizational corruption, breach of trust, and asset misappropriation. However, during the legislative deliberation of the Public Interest Whistleblower Protection Act enforced in 2025, all provisions pertaining to the "private sector" were excised from the draft bill. Lacking mandatory statutory protections, private sector employees reporting corruption or fraud within their own companies face dismissal and personal perils, including termination resulting in complete loss of livelihood, as well as the threats to retaliatory litigation and personal safety. Reporting against corporate executives places private employees at extreme risk, constituting a profound violation of the core spirit of Article 33 of the United Nations Convention against Corruption (UNCAC).

2.2 Recommendations

2.2.1 Initiate Phase II Amendments to Incrementally Mandate Private Sector Protection under the Act

The legislature must discard the passive mindset that "statutory regulation of the private sector would excessively interfere with corporate governance and significantly increase personnel management costs." Without a substantive legal shield, employees may remain silent due to pressures regarding livelihood, accomplice structures, and corporate retaliatory litigation, thereby creating a major vulnerability in the anti-corruption legal framework. Taiwan should expeditiously amend the Public Interest Whistleblower Protection Act to comprehensively cover both the public and private sectors, enforcing whistleblower identity confidentiality and anti-retaliation mechanisms. Furthermore, for private sector entities reaching a specified threshold—such as public companies, TWSE/TPEX listed enterprises, and regulated financial franchises—the establishment of internal whistleblowing systems should be legally mandated.

2.2.2 Develop De-Identified "Guidelines for Anonymous Whistleblowing Intake and Investigation" in both Public and Private Sectors

Competent authorities should formulate strict, operational "Technical Guidelines for Anonymous Whistleblowing Intake and Investigation" incorporating de-identification measures for both public and private sectors. These guidelines should explicitly mandate that reporting channels be structurally isolated from executive management, and that receiving units (such as independent Audit Committees or external third-party professional forensic teams) possess statutory independence. Substantive confidentiality and security must be guaranteed throughout the entire lifecycle of intake, recording, and record retention, integrated with digital platforms and

AI for high-risk keyword identification and pattern monitoring.

2.2.3 Mandate the Embedding of Internal Whistleblowing Mechanisms into Corporate Governance Evaluations and Internal Control Regulations

Competent authorities should formally incorporate "the implementation of internal whistleblower protection and anti-retaliation clauses" as mandatory audit items and governance evaluation criteria under the Regulations Governing Establishment of Internal Control Systems by Public Companies. This will guide enterprises to revise internal personnel regulations, adopt anti-retaliation clauses, and comprehensively reference the international ISO 37002 "Whistleblowing management systems — Guidelines" as a standardized framework for private sector transition, thereby building proactive integrity-based corporate governance.

3. Promote the Establishment of Corporate Anti-Corruption Committees

3.1 Observations and Findings

3.1.1 Private Sector Anti-Corruption Governance Remains Formalistic, Lacking Integrated Governance Capabilities

While most enterprises have incorporated governance structures such as Chief Corporate Governance Officers, legal compliance units, or internal audit units, and have gradually introduced internal control systems with basic compliance and audit functions, these capabilities are largely formalistic—focusing on information disclosure, regulatory compliance, or documentation. They generally lack substantive capabilities to integrate risk assessment, internal reporting, investigation handling, and horizontal coordination.

In anti-corruption and anti-bribery, most enterprises rely on decentralized management, where procurement, legal, and audit departments operate independently without a unified governance framework led by the board of directors or senior management. Furthermore, existing reporting and investigation mechanisms are often confined to traditional grievance systems, lacking dedicated and independent units for systematic analysis and follow-up tracking, which prevents the effective integration of risk identification and response mechanisms. Taiwan's integrated, professional, and independent anti-corruption governance still has room for enhancement and does not yet fully meet international expectations for corporate anti-corruption mechanisms.

3.1.2 Inadequate Due Diligence on External Business Partners, Presenting Significant Risks in Cross-Border and Public Procurement Transactions

Enterprise risk management over external business partners (suppliers, contractors, and partners) relies excessively on basic contract clauses or written declarations, lacking substantive risk assessment, due diligence, and risk-tiered management mechanisms. Particularly for enterprises undertaking public procurements or engaging in cross-border transactions, the risks of bribery and improper benefit transfers are significantly heightened, yet effective risk control mechanisms remain absent.

3.1.3 Over-Reliance on "Soft Advocacy" to Promote Anti-Corruption Policies, Lacking Structural Regulatory Constraints and Incentives

Due to commercial concerns over "reputation" and "stock prices," private enterprises generally exhibit low willingness to actively seek public sector or judicial assistance for internal corruption cases. However, in responding to the private sector's passive anti-corruption stance, the government heavily relies on soft governance evaluations and promotional measures (e.g., conducting 84 corporate integrity forums, 700 anti-corruption lectures, compiling integrity manuals and digital learning materials), lacking structurally binding regulatory frameworks and supporting legal and regulatory measures.

3.2 Recommendations

3.2.1 Mandate or Guide Enterprises of a Specified Scale to Establish Dedicated "Anti-Corruption Committees"

The government should require through legislative mandate, or incentivize through policy guidance, enterprises meeting a certain scale or criteria (such as TWSE/TPEX listed companies or government procurement contractors) to set up a dedicated anti-corruption governance body overseen by the board of directors or senior management: an "Anti-Corruption Committee", and incorporate this into Corporate Governance Evaluations (ESG indicators) as bonus criteria.

"Anti-Corruption Committee" will oversee corporate anti-corruption policies, external partner risk management, and internal reporting mechanisms, horizontally integrating internal control and anti-fraud functions to overhaul current fragmented management practices. Its members should possess cross-disciplinary professional backgrounds (e.g., lawyers, CPAs, CFEs) to enhance professionalism and independence. Referencing UK and OECD framework designs, establishing an Anti-Corruption Committee can integrate risk assessment, internal control systems, and investigation functions, mitigate private sector bribery risks, strengthen internal controls and disclosure, and establish a normative foundation for corporate liability.

3.2.2 Guide Corporate Self-Regulation and External NGO Oversight to Jointly Build Binding Enforcement

The government should establish substantive structural incentives (e.g., voluntary disclosure penalty mitigation or exemption) to alleviate private sector reputational concerns, guide enterprises to reference benchmark self-regulation cases, and encourage the private sector to shift from a passive to a proactive anti-corruption stance. For instance, referencing Taiwan Semiconductor Manufacturing Company's (TSMC) Audit Committee "Complaint Policy and Procedures," enterprises should build sound, independent internal control mechanisms that permit anonymous reporting and strictly prohibit retaliation.

Furthermore, in advancing anti-corruption policies, the government should actively collaborate with non-profit organizations composed of industry, government, academia, and legal experts (CPAs, lawyers, prosecutors, investigators, and law enforcement officers)—such as CPA associations, Bar associations, and the ACFE Taiwan Chapter—to leverage external oversight, professional training, and diverse technical exchange. Public-private partnerships can foster a "zero-corruption" organizational culture and create an enforceable anti-corruption mechanisms

4. Structure a Comprehensive Framework for Corporate Criminal Liability

4.1 Observations and Findings

4.1.1 Corruption Crimes Shift towards "Organizational Crime": Traditional Individual Attribution Models Fail

In modern economic activities, major fraud and corruption offenses are rarely isolated acts of individual natural persons; rather, they constitute "organizational wrongdoing" arising from complex collective decision-making or deliberate internal control omissions fostered by corporate cultures pursuing "profit maximization." Taiwan's legal framework has long adhered to the Civil Law principle of "liability based on conduct" (individual-responsibility model), holding that only natural persons possess criminal capacity. This mindset, which excessively focuses on individuals and predicates liability on natural-person offenses, fails to effectively address modern corporate structural crime.

4.1.2 Current Sanction Dilemmas of Corporate Corruption Liability: Imbalance and Impunity

The current legal framework provides for a "dual-penalty system"—punishing both the natural person and imposing a fine on the legal person—only within specific special criminal statutes such as the Banking Act, Money Laundering Control Act, Trade Secrets Act, and Act Governing Food Safety and Sanitation, lacking a comprehensive standalone corporate criminal liability framework. Because the law does not recognize legal persons as independent criminal subjects or suitable entities for confiscation, combined with the principle prohibiting multiple punishments for the same act, corrupt enterprises in practice often retain their illicit gains after paying criminal fines. Consequently, corporate conduct and criminal sanctions are severely disproportionate, allowing legal persons to escape unscathed without true criminal accountability—a clear injustice.

4.2 Recommendations

4.2.1 Construct an Independent and Comprehensive Chapter on Corporate Criminal Liability in the General Provisions of the Criminal Code

A sound anti-corruption regime must account for both natural and legal persons. The legislature should first recognize that legal persons possess independent criminal capacity and may be subject to punishment and confiscation. An independent and comprehensive chapter on corporate criminal liability should be constructed within the General Provisions of the Criminal Code, formally establishing legal persons as subjects of criminal prosecution and confiscation. Uncoupling corporate criminal liability from that of natural persons is essential to combat recurring economic crimes and prevent systemic corruption within organizational structures.

4.2.2 Introduce the Attribution Theory of "Organizational Defect" via Legislation

Drawing upon the legislative spirit of the UK Bribery Act, the legal person should be deemed to have an “organizational defect” and held independently criminally liable, where an employee or agent of a legal person commits an offense involving corruption, non-arm's length transactions, or impairment of fair competition, if the legal person is proven to have "failed to establish reasonable and necessary preventive measures" or exhibits "internal supervisory omissions lacking legal compliance mechanisms". This would create a powerful legal incentive for legal persons to proactively reinforce supervisory duties and implement compliance workflows. Furthermore, referencing legislative precedents such as the French Penal Code, for legal persons committing major corruption, related-party asset stripping, or transnational bribery, criminal or non-criminal sanctions should extend beyond monetary fines to include deterrent non-monetary sanctions, such as "dissolution orders", "debarment or suspension from specified government procurement opportunities", and "restrictions on advertising or specific business activities".

5. Establish a Comprehensive Reporting and Disclosure System for Beneficial Ownership Information

5.1 Observations and Findings

5.1.1 Complex Corporate Ownership Structures Obscure Ultimate Beneficial Owners

The key to maintaining capital market order and deterring corruption lies in the real-time, transparent identification of the natural persons exercising ultimate control behind the scenes. However, in Taiwanese practice, "corporate shareholders" serving as directors or supervisors is an exceptionally widespread phenomenon. These corporate shareholders are often structured through multi-layered cross-shareholdings and offshore shell companies in tax havens. Consequently, when judicial authorities investigate major insider trading or related-party transactions, penetrating the corporate veil to identify the "ultimate beneficial owners" exercising a controlling position proves exceedingly difficult.

5.1.2 Existing Framework Relies on "Formal Equity Reporting," Lacking Substantive Control Identification

Under the existing system, the Ministry of Economic Affairs (MOEA) maintains a reporting platform pursuant to Article 22-1 of the Company Act, where the reporting threshold is set at major shareholders holding over 10% of shares. Meanwhile, sector-specific anti-money laundering regulations maintain fragmented standards for identifying beneficial owners, mostly defaulting to a formal 25% shareholding threshold. International bodies such as the Financial Action Task Force (FATF), the European Union, and Singapore generally require the establishment of a publicly accessible "Centralized Registry for Ultimate Beneficial Owners (UBO)" to lay a normative foundation for identifying "natural persons exercising ultimate control over the company." This contrasts sharply with Taiwan's current reliance on "formal equity registration" criteria, preventing competent authorities from acquiring adequate and accurate beneficial ownership information and resulting in a severe decoupling from international practice.

5.2 Recommendations

5.2.1 Comprehensively Amend Article 22-1 of the Company Act to Incorporate the UBO Penetration Principle

The Company Act has historically failed to mandate the disclosure of ultimate beneficial ownership information by legal persons, allowing natural persons holding ultimate control to hide behind the corporate veil to evade legal liability. The MOEA should rapidly amend the Company Act, discarding purely formal equity criteria (10% or 25% shareholding) as sole benchmarks, and adopting natural-person concepts based on substantive control, voting trusts, and other ultimate-control relationships. The law should mandate that legal

社團法人台灣舞弊防治與鑑識協會　　立案字號：台內團字 1040073181 號
會址：103 台北市大同區長安西路 66 號 2 樓之 1　　電話：02-2556-5988　傳真：02-2556-7089
網址：http://www.acfetaiwan.org.tw　　Email: secretary@acfetaiwan.org.tw

entity structures be looked through layer by layer until reporting reaches the "natural person with ultimate controlling power," transforming the current system from superficial "major shareholder reporting" into an internationally aligned "Ultimate Beneficial Owner (UBO) Look-Through Registration System". The Financial Supervisory Commission (FSC) should likewise require public companies to look through multi-layered corporate shells to substantively disclose the "ultimate controlling persons" behind major shareholders, directors, and supervisors, preventing controlling figures from hiding behind the corporate veil to evade legal accountability.

5.2.2 Introduce Corporate Role-holder Identifiers(CRI) and Flexible Public Disclosure Mechanisms

The MOEA should integrate the existing "Major Shareholder Information Reporting Platform" and the "Commercial Regulations Information Public Query System," introducing a "Corporate Role-holder Identifier(CRI)" mechanism to assign digital personal identification codes across systems for all corporate directors, managers, and general partners of limited partnerships. Furthermore, to balance personal data protection with the public's right to know, a "flexible disclosure policy" should be adopted, granting access only to members of the public and financial institutions meeting specific legitimate interest criteria. Information transparency can operate as an ex ante preventive mechanism by making ownership and control structures visible and reducing opportunities for organizational money laundering and related-party fraud.

6. Improve Judicial Transparency by Disclosing Forensic Accounting and Appraisal Reports in Full

6.1 Observations and Findings

6.1.1 Shadows beneath the Sunshine Laws: Critical Core Information Remains an "Opaque Black Hole"

Taiwan has constructed the foundational legal transparency framework of the "Four Sunshine Laws" (Public Servant Asset Declaration, Recusal Due to Conflicts of Interest, Political Donations, and Lobbying Acts), and judicial reforms have progressively implemented the public disclosure of judgments and indictments to combat corruption through administrative transparency and rebuild public trust. However, the full texts of "appraisal reports" and "expert witness opinions"—which play a pivotal role in court proceedings—remain entirely excluded from proactive public disclosure. Courts often include only fragmentary excerpts of appraisal conclusions in their judgments. Consequently, the general public, academic institutions, and interested parties are unable to examine the deductive reasoning, calculation models, and underlying empirical data of these professional reports, leaving them as shadows beneath the sunshine laws.

6.1.2 Strict File Inspection Thresholds Obstruct Information Disclosure, Lacking Adequate Judicial Remedies

The existing Court Organization Act only regulates the public disclosure of written judgments, excluding "litigation files" (such as the full text of appraisal reports). Furthermore, constrained by the strict limitations of Article 242, Paragraph 2 of the Code of Civil Procedure, third parties who are non-litigants must obtain consent from the parties involved or demonstrate a legal interest, subject to court approval, to petition for file inspection. This statutory restriction prevents the public and academic institutions from evaluating the quality of valuation and appraisal reports. When disclosure is refused, the available remedies are an administrative appeal and administrative litigation under the Freedom of Government Information Law. The existing framework provides even less effective means of sanctioning those who issue false reports.

6.2 Recommendations

6.2.1 Proactively Disclose the Full Text of Appraisal and Expert Reports in Principle

Article 83 of the Court Organization Act and relevant procedural laws should be amended to explicitly mandate that, upon the termination of litigation proceedings (when a judgment becomes final), the court shall proactively publish the full text of "appraisal reports" and "expert witness opinions" cited in individual cases in a de-identified digital format on official platforms, except for matters involving national secrets, highly intimate personal information, or core trade secrets. This would alter the closed status quo where judges merely provide fragmentary excerpts of conclusions in written judgments, allowing the public and academic institutions to comprehensively examine the deductive reasoning and data of such reports to achieve substantive judicial oversight.

6.2.2 Impose Severe Sanctions on False Private-Sector Valuation and Appraisal Reports

Regarding major asset-stripping scandals involving related-party mergers and acquisitions or sales of assets under fair value, improper conduct by private professional institutions (such as CPAs, appraisers, and valuation bodies) intentionally issuing false evaluation reports must be severely sanctioned. Policy-wise, the professional capacity of law enforcement personnel—including police, prosecutors, and investigators—to read and analyze valuation and appraisal reports should be systematically cultivated. Furthermore, digital forensics capabilities within law enforcement agencies should be strengthened, enabling them to utilize forensic tools to accurately detect fraudulent valuations, as well as complex money laundering and corruption schemes.

7. Utilize Automation and AI Technologies to Enhance the Capabilities of Corruption Prevention and Investigation

7.1 Observations and Findings

7.1.1 Current Risk Management Mechanisms Lack a Highly Standardized, Data-Driven "Dedicated Systemic Anti-Corruption Risk Assessment Methodology"

According to the ACFE 2024 global occupational fraud survey report, global organizations lose an average of approximately 5% of their annual revenues to fraud, with nearly half of these cases involving corrupt activities, underscoring the widespread prevalence of fraud and corruption risks. Among fraud cases occurring in government sectors, 56% involve corruption, indicating that corruption risks are particularly pronounced in public agencies. Taiwan's government agencies primarily rely on the current "Integrated New System for Risk Management (including Internal Control) in Government Agencies" and routine operations by ethics units (such as Integrity Report Meetings and special project audits).

However, this framework leans heavily toward decentralized self-management and sampling audits, lacking a nationally consistent, highly standardized, and data-driven "dedicated systemic anti-corruption risk assessment methodology." Furthermore, the "Crystal Transparency Award"—one of the core showcases of effectiveness—remains voluntary in nature (with only 79 agencies participating over three editions), making it incapable of mandating universal systemic risk assessments across all high-risk agencies.

Although certain government agencies have begun introducing data analytics tools—for example, the National Audit Office has developed programs connected to the Government e-Procurement System to detect anomalous transactions and filter risks via automated query and analysis, showing that Taiwan is progressively advancing toward digital auditing—overall, cross-agency data integration, real-time monitoring mechanisms, and AI model applications have not been fully institutionalized, leaving significant room for improvement. Relying solely on institutional design without integrating effective detection and prevention tools renders traditional controls more vulnerable to bypass or failure in an AI-driven environment, while post-incident detection and investigation may also be unable to identify complete transaction trails.

7.1.2 Advances in AI Technology Present Major Challenges to Traditional Audit Mechanisms and Investigative Techniques

With the rapid development of artificial intelligence (AI) technology, fraud methodologies have undergone significant evolution. Fraudsters have begun deploying tools such as generative

AI to forge increasingly sophisticated and hard-to-detect transaction documents and records, examples include forged contracts, invoices, bank statements, and email communications, and even simulated end-to-end transaction processes and fund flows. Such technologies drastically enhance the covert nature of fraudulent conduct, posing severe challenges to traditional document-centric internal control mechanisms and increasing the difficulty of investigation and identification, thereby exerting emerging risk pressures on the existing anti-corruption system. Currently, the financial sector has progressively introduced AI and data analytics technologies into anti-money laundering and behavioral monitoring mechanisms, establishing a relatively mature operational model. Practice has evolved from traditional rule-based systems to anomaly detection frameworks integrating machine learning and AI models, enhancing suspicious transaction reporting efficiency and reinforcing internal behavioral monitoring. In contrast, a noticeable gap persists in AI adoption across other industries and government agencies.

7.2 Recommendations

7.2.1 Prioritize the Deployment of AI Monitoring Mechanisms in High-Risk Industries and Government Agencies

Competent authorities should adopt a phased implementation strategy aligned with the spirit of Article 5 of the United Nations Convention against Corruption (UNCAC). For the private sector, high-risk industries such as energy, high-tech, and manufacturing should be prioritized for encouragement and guidance. For the public sector, automated and AI-assisted monitoring and analytics tools should be introduced across high-risk government functions and entities, including public works, public procurement, state-owned enterprises, and subsidy fund management—to enhance real-time identification and early warning capabilities for anomalous transactions, improper benefit transfers, and other corrupt practices.

7.2.2 Establish a Cross-Agency Data Integration and Shared Platform

Promote cross-agency data linkage and integration to construct a unified data platform, improving data usability and completeness to support AI models in multi-dimensional analysis. This will strengthen risk identification capabilities across transactions and cases, elevating the overall effectiveness of fraud risk management.

7.2.3 Institutionalize AI and Data Analytics Technologies into Investigative and Monitoring Mechanisms

Formally incorporate AI technologies—including data integration and analytics, anomaly detection, link network analysis, and behavioral pattern analysis—into the statutory framework of investigative and monitoring tools. Drive a strategic transition from post-incident auditing to continuous monitoring and pre-emptive warning mechanisms, while providing AI-related training for investigative, audit, and supervisory personnel to enhance identification precision regarding organizational and systemic corruption.

7.2.4 Establish Frameworks for AI Governance, Oversight, and Evidentiary Admissibility

Taiwan passed the Artificial Intelligence Basic Act at the end of 2025, and competent authorities have issued corresponding guidelines. As AI applications expand into law enforcement and anti-corruption investigations, a comprehensive AI governance and oversight framework should be further constructed, covering model transparency, data quality management, algorithmic bias control, and accountability mechanisms. Simultaneously, clear regulations must govern the utilization of AI analysis results in administrative and judicial proceedings to ensure their legality, credibility, and evidentiary admissibility.

8. Accelerate the Statutory Authorization for Special Compulsory Investigative Measures

8.1 Observations and Findings

8.1.1 Excessive Sluggishness in Codifying Technology-Driven Investigations Severely Impairs Law Enforcement Efficiency

According to the normative spirit of special investigative techniques under Article 50 of the United Nations Convention against Corruption (UNCAC), law enforcement agencies must be equipped with investigative authorizations that keep pace with technological advancements in order to effectively combat cross-border, highly covert major corruption and money laundering crimes. However, as early as 2017, in Supreme Court Criminal Judgment No. 106-Tai-Shang-3788 (2017), the Court dismissed the appeal from the judgment of the Taichung Branch of the Taiwan High Court, establishing the rule that installing GPS tracking devices—even for the necessity of criminal investigation—constitutes an unlawful act lacking statutory basis, and in judicial practice even forms an offense against privacy under the Criminal Code. Regarding the Undercover Investigation Act, official authorities reached a passive, entirely negative conclusion citing practical operational hurdles such as personnel safety, identity protection, criminal immunity, and evidence evaluation, determining that "it is currently inappropriate to pursue," which brought related legislation to a complete standstill.

In terms of tech investigations, official authorities effectively abandoned the originally planned standalone Science and Technology Investigation Act, opting instead for a compromise by adding a dedicated chapter to the Code of Criminal Procedure. On July 16, 2024, Taiwan's Code of Criminal Procedure was amended to formally add the chapter on "Special Compulsory Measures," finally providing explicit statutory authority for technology-driven investigative methods such as GPS positioning, IMSI-catcher vehicles (commonly referred to in Taiwan as “M-vehicles”), real-time location tracking, and non-physically intrusive video surveillance of private spaces. Nevertheless, doubts persist as to whether this partial amendment fully covers cross-border digital legal mechanisms for "obtaining evidence and intelligence from computer systems during authorized investigations" as specified in the Convention and International Review Recommendations.

From the Supreme Court's ruling substantially blocking technology-driven investigations to the Legislative Yuan's formal completion of the Special Compulsory Measures legislation in 2024, the process suffered a delay of seven full years. During these seven years of statutory vacuum, frontline investigators faced high legal exposure and liability while confronting the digitization of corrupt cash flows, leaving investigative techniques severely lagging behind technological developments.

8.1.2 Narrow Scope of Current Statutory Authorization Fails to Address the Technological Reality of Encrypted Communications

Under the 2024 amendments, the scope of application for Special Compulsory Measures remains strictly limited to "public places and non-intrusive" investigative methods. Considering that contemporary criminal syndicates and corrupt officials accepting bribes have long abandoned traditional telephony in favor of end-to-end encrypted messaging applications (such as LINE, Signal, WhatsApp and Telegram) to coordinate stories, tamper with evidence, and arrange illicit benefit transfers, existing communications surveillance (wiretapping) techniques are entirely incapable of intercepting real-time content during the use of such encrypted software. Even when suspects' smartphones are lawfully seized post-incident, suspects frequently refuse to provide unlock passcodes, preventing law enforcement agencies from accessing the devices. Although police and prosecutors' offices are equipped with digital forensic unlocking and extraction tools, in practice, owing to mobile operating system updates and the robust security settings of messaging applications, many smartphone passcodes cannot be cracked, nor can deleted chat logs be restored. If perpetrators rely exclusively on voice calls, law enforcement agencies face a complete deadlock in securing core critical evidence.

8.2 Recommendations

8.2.1 Accelerate Explicit Legislation for "Intrusive Technology Investigation Techniques"

To thoroughly fulfill the spirit of special investigative techniques under UNCAC Article 50, the legislature should not be satisfied with current compulsory measures that are strictly confined to public places and non-intrusive methods. For major corruption, cross-border kickbacks, and money laundering crimes, the legislature should accelerate the review and enactment of explicit statutory provisions authorizing more intrusive technology investigation techniques. For example, upon obtaining a court-issued technology investigation warrant (or search warrant), law enforcement agencies should be explicitly authorized to send specially configured shortened URLs or deploy specific Trojan programs (remote communications surveillance software) onto target devices, directly capturing real-time chat logs and voice communications from endpoint devices behind encrypted messaging software, thereby breaking digital defense barriers.

8.2.2 Implement a Strict Judicial Warrant Requirement and Tiered Control Mechanism

Regarding intrusive technology investigation techniques, statutory regulations must incorporate procedural rules stricter than those governing GPS tracking. A prior judicial warrant requirement (judicial reservation principle) must be universally applied, requiring prosecutors to demonstrate to the court that strong suspicion of crime exists and that no alternative investigative means are available (principle of last resort / subsidiarity) before a judge may issue a time-limited implementation warrant. Furthermore, Standard Operating Procedures (SOP) for digital forensic personnel operating such software must be explicitly codified to guarantee the digital-native authenticity and chain of custody/traceability of obtained evidence.

9. Enact the Virtual Asset Supervision Act and Enforce the Travel Rule

9.1 Observations and Findings

According to the Association of Certified Fraud Examiners (ACFE) Occupational Fraud 2026: A Report to the Nations, while emerging financial technologies provide great convenience, they also frequently serve as money laundering vehicles for concealing criminal proceeds and facilitating cross-border transfers in corruption cases. Fueled by AI and virtual currencies, white-collar economic crimes and commercial bribery in Taiwan utilizing virtual currencies for transactions or money laundering have shown a significant upward trend in recent years. In judicial practice, multiple major bribery cases (some even involving national security and disclosure of official secrets) have emerged in Taiwan where virtual currency was used as consideration. However, an examination of the government's current control mechanisms over Virtual Asset Service Providers (VASPs) reveals three major regulatory blind spots:

9.1.1 Misplacement of Legal Basis Preventing Uniform Application to Corruption, Narcotics, and Other Crimes

Currently, the government's regulatory framework for VASPs—including pre-emptive controls on warning accounts, provisional restriction measures, cross-industry inquiries, and joint prevention reporting systems—is fragmentarily codified solely within the Fraud Crime Hazard Prevention Act (the "Anti-Fraud Special Act"). Consequently, when offenses fall under "non-fraud" categories, such as major corruption, official bribery, cross-border money laundering, or the transfer of illicit proceeds from narcotics trafficking, law enforcement agencies cannot invoke the joint prevention alert reporting and real-time fund hold controls provided under the Anti-Fraud Special Act. This creates severe regulatory fragmentation and enforcement loopholes.

9.1.2 The Core Safeguard of Anti-Money Laundering, the "Travel Rule," Has Yet to Be Implemented

The Financial Action Task Force (FATF) "Travel Rule" explicitly mandates that VASPs globally must obtain and transmit required originator and beneficiary information immediately and securely during virtual asset transfers. However, Taiwan has yet to fully implement the Travel Rule, making it exceptionally easy for blockchain transaction trails to suffer from information breakpoints during transfers.

9.1.3 Offshore Foreign VASPs Create a Massive Regulatory Blind Spot

Taiwanese citizens and criminal syndicates extensively utilize foreign, non-established, and unregistered VASPs (such as major offshore exchanges and decentralized wallets). Because these platforms refuse to cooperate with domestic law enforcement agencies in intelligence gathering and evidence procurement, immense regulatory hurdles and investigative blind spots persist.

9.2 Recommendations

9.2.1 Enact a Standalone Virtual Asset Supervision Act

The government should proactively enact an independent Virtual Asset Supervision Act that explicitly extends pre-emptive warning account controls, cross-sector notification, and provisional fund hold mechanisms uniformly across all predicate offense types—including offenses under the Anti-Corruption Act, Special Breach of Trust under financial statutes, and the Money Laundering Control Act—rather than downgrading virtual currency oversight to a subordinate position within the Anti-Fraud Special Act.

9.2.2 Mandate the Comprehensive Enforcement of the "Travel Rule"

The Financial Supervisory Commission (FSC) should impose a mandatory legal obligation on domestic VASPs that have completed AML registration, requiring them to rigorously enforce the Travel Rule during virtual asset transfers by transmitting and verifying the identified information of both transacting parties in real time. Furthermore, for unregistered offshore VASPs that refuse to comply with law-enforcement or judicial requests for information from Taiwan, the government should formulate stringent restrictions—such as domain name blocking (IP/DNS filtering) and prohibiting financial institutions from processing credit card fiat-on-ramp deposits—to sever illicit cash flows and plug offshore regulatory blind spots.

10. Formally Include the "Certified Fraud Examiner (CFE)" Credential in the Qualification Requirements for Internal Auditors

10.1 Observations and Findings

10.1.1 The Government Actively Participates in Multilateral Organizations, Successfully Transforming Anti-Corruption Experience into Diplomatic Soft Power

In recent years, Taiwan has actively participated in regional multilateral bodies such as the Asia/Pacific Group on Money Laundering (APG) and the APEC Anti-Corruption and Transparency Experts Working Group (ACTWG), sharing expertise in anti-corruption, anti-money laundering, and asset recovery techniques. Through professional diplomacy, Taiwan has successfully overcome international constraints and achieved fruitful outcomes in international exchanges, which fully aligns with the spirit of technical assistance and experience sharing enshrined in the United Nations Convention against Corruption (UNCAC).

10.1.2 A Missing Link in International Technical Exchange: Statutory Qualifications Omit Globally Authoritative Anti-Fraud Credentials

Under the authorization of Article 11 of the Regulations Governing Establishment of Internal Control Systems by Public Companies, the Securities and Futures Bureau of the Financial Supervisory Commission (FSC) prescribes the statutory qualification requirements for internal auditors. Currently, these qualification standards only recognize passing the examinations for Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), and domestic Certified Public Accountant (CPA) as statutory professional certifications eligible for waiving baseline entry-level seniority requirements, regrettably omitting the globally authoritative Certified Fraud Examiner (CFE) credential, which carries significant influence in the global anti-corruption field. The CFE examination integrates core subjects including Financial Transactions and Fraud Schemes, Fraud Investigation Law and Techniques, and Fraud Prevention and Deterrence. Including this credential would significantly cultivate internal auditors' capabilities in fraud detection and deterrence, thereby strengthening the anti-corruption functions of private-sector audit departments.

10.2 Recommendations

10.2.1 Formally Include the CFE Credential in the Qualification Requirements for Internal Auditors

It is recommended that the Securities and Futures Bureau of the Financial Supervisory Commission (FSC), the competent authority for public companies, amend the administrative directive on the "Regulations Governing Qualification Requirements, Continuing Education and Training Hours for Internal Auditors and Their Deputies of Public Companies" to formally list individuals who have obtained the Certified Fraud Examiner (CFE) credential as meeting the statutory qualification requirements for internal auditors. Placing the CFE credential alongside Certified Public Accountants (CPAs), Certified Internal Auditors (CIAs), and Certified Information Systems Auditors (CISAs) will enhance fraud prevention capabilities within private-sector audit functions and align with international anti-fraud methodologies.

10.2.2 Leverage Professional Networks of International NGOs to Strengthen Public and Private Sector Education and Training in Fraud Prevention and Anti-Corruption

Fraud risk management is an integral component of internal control. The government should work with civil society and globally recognized professional associations such as ACFE Taiwan Chapter to provide nation-wide education and training in fraud prevention and anti-corruption governance across both public and private sectors. The government should promote a model of "Soft Power Technical Resource Sharing" to popularize cross-disciplinary CFE professional training. This will substantively integrate CFE methodologies—including fraud identification, fraud investigation, and fraud prevention/deterrence techniques—into the operational practices of national law enforcement agencies (prosecutors, police, investigators, and ethics officers) and the private sector.

Taiwan Anti-fraud and Forensic Accounting Association (ACFE, Taiwan Chapter)

http://www.acfetaiwan.org.tw
secretary@acfetaiwan.org.tw