

Regulatory Measures Regarding Security Token Offering in Decentralized Systems for Combatting Money Laundering in Thailand

Yosita Saikhwan¹, Khwanmanee Maneechot^{2*}, Kanokphol Nikornpest³

^{1,2,3} School of Law, Center of Geosocial and Cultural Research for Sustainable Development (GSCR), Walailak University, Thailand

*Corresponding Author: kwanmanee.ma@wu.ac.th

Citation: Saikhwan, Y., Maneechot, K. & Nikornpest, K. (2025). Regulatory Measures Regarding Security Token Offering in Decentralized Systems for Combatting Money Laundering in Thailand, *Journal of Cultural Analysis and Social Change*, 10(4), 2375-2387. <https://doi.org/10.64753/jcasc.v10i4.3229>

Published: December 13, 2025

ABSTRACT

This research undertakes a comparative analysis of Thailand's anti-money laundering ("AML") regulatory framework in relation to the most recent recommendations issued by the Financial Action Task Force ("FATF") concerning money laundering risks associated with Security Token Offerings ("STOs") conducted via blockchain technology. The objective is to identify potential regulatory gaps and areas for improvement in Thailand's existing AML measures, particularly in the areas of regulatory oversight, licensing requirements, customer due diligence ("CDD"), recordkeeping obligations, and the reporting of suspicious transactions by virtual asset service providers ("VASPs"). The methodological basis of the research is the comparative analysis method, examining Thailand's applicable AML laws and regulations alongside FATF guidelines, relevant literature, and case law. The research found that Thailand's applicable AML laws, including the relevant regulations, are inadequacies and inefficiencies in the regulatory oversight of securities offerings that utilize emerging technologies. Specifically, the current regulatory framework is insufficient in effectively preventing or mitigating risks related to money laundering and the financing of terrorism for investors. As a result, it does not adequately ensure the security and integrity of investments in decentralized systems, therefore, it fails to provide sufficient safeguards to protect investors from inadvertently becoming involved in unlawful activities. These shortcomings indicate a lack of alignment with international standards issued by the FATF. This research is useful to legislative authorities, lawyers, law students, and regulatory bodies, especially in Thailand, and only limited to the regulation of money laundering in Thailand and does not provide empirical research.

Keywords: Money laundering, Security Token Offering, Blockchain technology, Customer due diligence, Virtual asset provider, Suspicious transactions.

INTRODUCTION

The explosive development of blockchain technology and the creation of decentralized financial systems have had an important impact on the global capital markets. Among these innovations, Security Token Offerings have been developed as a revolutionary fundraising technique that digitizes traditional securities through distributed ledger technology ("DLT"). STOs offer enhanced efficiency, transparency, and accessibility to customers in the case of issuers and investors. However, these gains are bound by major regulatory obstacles, especially in terms of money laundering risks in decentralized environments. (Zohar, 2020).

In Thailand, the regulatory landscape surrounding STOs is still evolving. The principal legal instruments governing digital assets are the Emergency Decree on Digital Asset Businesses B.E. 2561 (A.D., 2018), the Anti-Money Laundering Act B.E. 2542 (A.D., 1999), and Counter-Terrorism and Proliferation of Weapon of Mass

Destruction Financing Act B.E. 2559 (A.D., 2016), as amended. These laws were designed primarily to regulate centralized digital asset exchanges and service providers and thus may not be sufficiently equipped to address the emerging risks associated with decentralized finance (“DeFi”) platforms and blockchain-based securities issuance (Securities and Exchange Commission (SEC), Thailand, 2021). Additionally, there is concern that the existing regulatory measures do not yet provide comprehensive mechanisms to ensure effective supervision, enforce compliance, or facilitate international cooperation in combatting money laundering for STOs.

Given the expanding adoption of digital assets and Thailand's aim to become a regional digital finance hub, the country's legal and regulatory frameworks shall adapt in accordance with global standards. The FATF, as the global standard-setter for anti-money laundering and counter-terrorist financing (“AML” and “CFT”), has issued specific recommendations for virtual asset service providers (“VASPs”), including those involved in STOs. These recommendations emphasize risk-based supervision, licensing, customer due diligence (“CDD”), recordkeeping, and the obligation to report suspicious transactions (FATF, 2023). This research attempts to critically evaluate Thailand's existing AML regulatory framework in relation to STOs and decentralized systems. By performing a comparative legal analysis of Thai legislation and the recent FATF guidelines, the research finds the regulatory gaps, legal contradictions, and practical implementation issues and also proposes strategic recommendations for improving the AML regime in Thailand and blending it with international standard practices. As a result, it contributes to the discussion of creating robust legal frameworks that not only prevent Thailand's financial system and Thai investors but also encourage innovation and cross-border compliance in the digital economy.

BACKGROUNDS

Security Token Offerings (STOs)

Security Token Offerings are a game-changing financial innovation that combines classic security principles with current blockchain technology. An STO is a method of raising capital through the issuance of security tokens, which are digital representations of real-world assets or financial instruments, such as stocks, bonds, or real estate properties. These tokens are created and offered on blockchain systems, with higher levels of transparency, liquidity, and efficiency than traditional means of securities trading. At its core, a STO serves as a regulated fundraising method in which security tokens represent ownership or a share of an underlying asset. Unlike Initial Coin Offerings (“ICOs”) (Auer & Weber, 2020), which often issue utility tokens that may not be backed by tangible assets or subject to regulatory oversight, security tokens are governed by existing securities laws. This shows that STOs provide a more secure and regulated option for relevant issuers to acquire funds while giving investors with more protection, as these STOs must comply with the same regulatory frameworks as regular securities offerings (Ganne, 2020).

How Security Token Offerings Work

The process of launching an STO involves several key steps:

- **Security Token Issuance:** A corporation or issuer issue a security token to represent an asset or ownership as subject to its business purpose. This digital token is constructed on distributed ledger technology (“DLT”), which provides transparency, immutability, and simplicity of transfer. Tokens can represent a variety of asset types, including stock, debt, and even tokenized physical assets such as real estate, gold, or commodities.
- **Regulatory Compliance:** STOs are subject to securities regulations, which vary depending on the jurisdiction. Issuers must comply with Know Your Customer (“KYC”) and AML requirements, ensuring that all participants in the offering are verified and that no illegal activities, such as money laundering or terrorist financing, take place.
- **Token Offering and Sale:** Once the token is designed and regulatory compliance is in place, the issuer conducts the offering. Investors can purchase the security tokens during the Token Sale phase, usually through a Private Sale or Public Offering depending on the issuer's goals and the applicable regulations.
- **Blockchain Infrastructure:** The tokens are typically issued on a public blockchain platform, such as Ethereum or Stellar, although private blockchains may also be used depending on the requirements of the issuer. The blockchain will make sure that transactions involving security tokens are transparently recorded and easily auditable, making it a safe channel for ownership transfer.
- **Liquidity and Trading:** After the offering, security tokens can be traded on regulated exchanges, ensuring that the tokens remain liquid. This is a significant advantage over traditional forms of securities, as blockchain technology enables faster and more efficient trading with fewer intermediaries (Minto, 2024).

Advantages of STOs

STOs have several advantages over traditional fundraising means, such as Initial Public Offerings (“IPOs”) or private equity placements:

- **Regulatory Compliance:** Since security tokens are subject to the same regulations as traditional securities, they provide investors with a higher level of protection compared to ICOs, which may not always comply with securities laws.
- **Liquidity:** Security tokens can be traded on global, decentralized exchanges, increasing liquidity and enabling investors to buy or sell their tokens more easily than with traditional assets.
- **Accessibility and Global Reach:** In contrast to traditional securities, which are regularly restricted by geographical borders, STOs can potentially be accessed by issuers and investors from anywhere in the world, opening up capital markets to a wider range of participants.
- **Transparency and Security:** Blockchain technology makes transparency and security by recording all transactions on an immutable ledger that everyone can access, resulting in a high level of confidence in the infrastructure.

STOs represent a hybrid model that blends traditional finance with cutting-edge blockchain technology. While offering significant advantages in terms of liquidity, transparency, and accessibility, STOs are subject to regulatory scrutiny to ensure investor protection and market integrity. The evolution in fundraising mechanisms provides a more trustworthy and effective way to traditional investment vehicles, as well as a bright future for digital assets and securities.

Anti-Money Laundering (“AML”)

Anti-money laundering refers to a set of laws, regulations, and procedures designed to prevent criminals from legitimizing illegally obtained funds. The fight against money laundering is a global priority due to its potential to facilitate serious crimes such as corruption, terrorism, and organized crime. Over the years, international bodies, such as the FATF, have played a crucial role in creating and promoting AML standards to ensure that financial institutions and other entities comply with global measures for detecting and reporting suspicious activities. Globally, FATF is the leading body responsible for developing and promoting global AML standards. Established in 1989, the FATF sets forth 40 Recommendations that provide the basis for AML laws in many countries. These recommendations cover a broad range of measures, including the need for KYC/CDD processes and the reporting of suspicious transactions. FATF also recommends that countries establish measures to prevent the misuse of financial institutions and services for criminal activities, including the implementation of strict reporting systems and cooperation between countries (FATF, 2023). A significant aspect of global AML is the risk-based approach advocated by FATF. This means that financial institutions must assess the risk of money laundering or terrorist financing in their operations and take appropriate steps to mitigate these risks. Over the years, the scope of FATF’s work has expanded to include emerging sectors such as virtual assets, reflecting the evolution of global financial markets and technology (FATF, 2023). Furthermore, international cooperation is a cornerstone of effective AML enforcement. Given that money laundering often involves cross-border transactions, international treaties and conventions are crucial. For example, the United Nations Convention against Transnational Organized Crime and the UN Convention against Corruption both promote global cooperation in preventing money laundering (United Nations, 2004).

In Thailand, AML laws have evolved in response to both international standards and the need to protect its financial system from abuse. Thailand’s AML framework is primarily governed by the Anti-Money Laundering Act B.E. 2542 (1999), which was amended in 2018 to improve compliance with FATF’s recommendations. The Anti-Money Laundering Office (“AMLO”) is the central authority responsible for enforcing AML regulations, investigating suspicious activities, and cooperating with other countries on international AML matters. Under Thailand’s Anti-Money Laundering Act, financial institutions, including commercial banks, securities firms, and insurance companies, are required to conduct CDD and KYC checking processes on their clients to verify their identities and assess the risks of their business relationships. Additionally, entities are obligated to report suspicious transactions to AMLO, and failure to comply with AML regulations can result in significant penalties (Securities and Exchange Commission, 2021). Thailand is also a member of FATF’s Asia/Pacific Group on Money Laundering (“APG”), and its regulations have aligned with international AML standards over the years. Thailand’s AML framework has improved in line with FATF’s recommendations, particularly in the areas of digital asset regulation. However, despite these advances, some gaps remain, particularly in regulating emerging technologies such as decentralized finance (“DeFi”) and Security Token Offerings. The rapid development of blockchain technology and cryptocurrency marketplaces caused concerns about Thailand’s capacity to effectively implement anti-money laundering laws and regulations in these new fields (Thailand AMLO, 2021). In recent years, Thailand has also introduced measures to prevent terrorist financing, hence improving its AML framework. By adopting a

risk-based approach, financial institutions and virtual asset service providers (“VASPs”) are required to assess the risk of money laundering and terrorist financing in their operations and to apply mitigation measures accordingly. The Thai government has emphasized the importance of international cooperation and information-sharing to tackle money laundering effectively across borders (Thailand FATF, 2021).

FATF RECOMMENDATIONS AND GLOBAL AML STANDARDS

The Financial Action Task Force (“FATF”) is an inter-governmental organization that sets global standards to combat money laundering, terrorist financing, and proliferation financing. FATF’s Recommendations are recognized as the global benchmark for AML and counter-financing of terrorism regulations. As the global financial landscape evolves, so too do FATF’s recommendations, which have increasingly focused on addressing the unique risks emerging from new technologies such as STOs and virtual assets. Thus, the FATF has progressively updated its recommendations to ensure that these emerging technologies are adequately regulated under global AML standards.

Keys of FATF Recommendations Regarding STOs

1. *Recommendation 1: Risk-Based Approach (“RBA”)*

FATF emphasizes the importance of a risk-based approach to AML, which is central to effectively regulating STOs. Jurisdictions and financial institutions are required to assess and mitigate the money laundering and terrorist financing risks associated with STO activities. In the context of STOs, this means understanding the specific risks posed by these offerings (e.g., anonymity, cross-border nature, and decentralized operation) and applying tailored AML measures accordingly.

2. *Recommendation 5: Customer Due Diligence (“CDD”)*

The implementation of CDD and KYC measures is critical in preventing money laundering and terrorist financing in STOs. FATF requires that platforms conducting STOs, or virtual asset service providers (“VASPs”), implement procedures to verify the identity of their customers and to assess the risks of their transactions. This process should include monitoring for unusual activity and reporting any suspicious transactions. The FATF recommends that these measures be adapted based on the risks identified through the RBA.

3. *Recommendation 10: Record-Keeping and Transaction Monitoring*

FATF mandates that VASPs, including those operating STO platforms, keep detailed records of all transactions for a minimum of five years. These records must be available to competent authorities and financial intelligence units (FIUs) for investigation and enforcement purposes. In the case of STOs, this means that all digital asset transactions must be thoroughly documented, with the necessary originator and beneficiary information securely retained.

4. *Recommendation 15: New Technologies and Virtual Assets*

As virtual assets like STOs are increasingly used for raising capital, FATF has issued specific guidelines for the regulation of these assets. FATF defines virtual assets as digital representations of value that can be used for investment or payment purposes and advises countries to regulate VASPs effectively to ensure compliance with AML/CFT measures. STO platforms fall under this category and are required to follow FATF’s standards, including the implementation of KYC and AML protocols, such as transaction monitoring and reporting.

5. *Recommendation 23: Regulation and Supervision of VASPs*

FATF requires that all VASPs, including STO platforms, be subject to effective regulation and supervision. This includes the obligation to obtain a license or registration with competent authorities, ensuring that platforms comply with all relevant AML/CFT obligations. Regulators are required to monitor these platforms through regular inspections, audits, and risk-based supervision to ensure ongoing compliance.

Challenges in Regulating STOs under FATF Recommendations

Despite the clear framework provided by the FATF, there are inherent challenges in applying these recommendations to STOs.

- 1. *Decentralization and Cross-Border Nature:*** One of the core challenges is the decentralized nature of blockchain technology, which allows STOs to operate across borders with minimal oversight. This raises significant concerns about the ability of regulators to trace illicit activities and enforce AML measures effectively. FATF’s risk-based approach helps address this by recommending that jurisdictions tailor their AML measures based on the specific risks posed by decentralized systems.

2. **Anonymity of Transactions:** The anonymity associated with virtual assets and blockchain transactions presents another challenge. FATF has addressed this issue by requiring STO platforms to implement strong KYC and CDD procedures to ensure that all investors are properly identified before participating in any offering. However, enforcing these requirements across jurisdictions with varying regulatory standards remains difficult.
3. **International Cooperation:** Since many STOs involve participants from multiple countries, **international cooperation** is critical for effective enforcement. FATF emphasizes the need for cross-border information sharing and collaborative efforts between national regulators to combat money laundering and terrorist financing in the realm of virtual assets.

The FATF Recommendations provide a comprehensive framework for regulating STOs and other virtual assets to prevent money laundering and terrorist financing. By applying a risk-based approach, FATF enables jurisdictions to tailor their AML measures to the specific risks posed by STOs. Despite the regulatory challenges, FATF's evolving guidance, particularly with regard to virtual assets, will play a key role in ensuring that STO platforms comply with AML/CFT requirements and contribute to the integrity of the global financial system. Effective enforcement will require international cooperation, robust supervision, and the application of technological solutions to track and prevent illicit activities in the digital asset space.

Laws And Regulations Regarding Anti-Money Laundering In Thailand

A comprehensive regulatory framework for the virtual asset market has been established in Thailand, ensuring that STOs are issued in compliance with Thailand's anti-money laundering regulations. STOs are regulated by the Thai government to prevent illegal financial transactions through the Anti-Money Laundering Office ("AMLO") and the Securities and Exchange Commission ("SEC"). This research provides a detailed analysis of the relevant AML laws, SEC regulations, and the compliance measures required for STO platforms operating in Thailand. The legal frameworks for AML in Thailand mainly have two Acts named (1) Anti-Money Laundering Act B.E.2542 (A.D.,1999) and (2) Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing Act B.E.2559 (A.D.,2016) which serve as the cornerstone of the country's efforts to combat money laundering. The AMLO is the primary regulatory authority responsible for enforcing the provisions of this Act, which applies to all financial institutions, including digital asset businesses. Additionally, in 2018, the Emergency Decree on Digital Asset Businesses B.E.2561 (A.D.,2018) was introduced, which specifically addresses the regulation of digital assets, including STOs. This order established a framework that requires securities or assets to follow AML and Counter-Terrorist Financing (CFT) legislation, making Thailand's laws in line with global standards issued by the FATF.

Key Provisions of Anti-Money Laundering Act B.E.2542 (A.D.,1999) and its Amendments

The Anti-Money Laundering Act in Thailand is a foundational piece of legislation aimed at preventing money laundering and terrorist financing. This law was enacted to comply with international AML/CFT standards, including those set by the FATF. The AML Act mandates the following obligations for entities operating within the financial sector, including STO platforms.

1) **Definition of Money Laundering:** Under the Anti-Money Laundering Act B.E.2542 (A.D.,1999), Section 3, money laundering is defined as the act of converting or transferring illegal proceeds or unfair securities trading practice under the law on securities and exchange or offense relating to unfair futures trading under the law on futures contracts or offense relating to unfair practice which affect the trading price of agricultural futures or the use of inside information under the law on agricultural futures trading. This AML Act aims to prevent the use of the financial system for illicit purposes, particularly drug trafficking, fraud, corruption, and terrorist financing. The law criminalizes any attempt to conceal or disguise the origin, ownership, or control of proceeds derived from criminal activities.

2) **CDD and KYC:** The requirement for CDD is a fundamental component of Thailand's anti-money laundering regulations. Under the AML Act, financial institutions, virtual asset service providers (VASPs), and STO platforms are mandated to verify the identity of their customers and assess the risks associated with them. This is in line with the KYC principle, which requires businesses to obtain and verify essential customer information. CDD/KYC requirements include

- Identification of Customers - financial institutions must obtain valid identification documents such as passports, national ID cards, or other official records to verify the identity of their clients.
- Verification of Beneficial Ownership Institutions for clients who are companies or legal entities - financial institutions must identify and verify the beneficial owners behind legal entities or organizations, particularly in cases where transactions involve companies or trusts.
- Assessment of Risk Profile - businesses are required to assess the risk associated with customers and transactions.

- Customers from high-risk jurisdictions or those involved in high-value transactions require enhanced due diligence measures (EDD).
- Ongoing Monitoring - regular reviews of customers' activities must be conducted to ensure they remain consistent with the institution's knowledge of the customer's business and risk profile. Any suspicious activity should be flagged for reporting to AMLO.

3) Reporting Suspicious Transactions (Suspicious Transaction Report, STR): Another important provision under the AML Act is the requirement for financial institutions to report any suspicious transactions to AMLO. This includes transactions that may be indicative of money laundering, terrorist financing, or other financial crimes. If a transaction is deemed suspicious, institutions must submit a Suspicious Transaction Report ("STR"), regardless of whether the transaction was completed or not. The AML Act specifies that financial institutions shall immediately report suspicious transactions to AMLO and withhold or delay the completion of transactions when there is reasonable suspicion that they involve illicit funds. In addition, financial institutions should cooperate with relevant authorities to provide additional relevant documents or details related to the suspicious transaction for investigation purposes. If financial institutions fail to report suspicious activities, these can lead to severe penalties, including fines or criminal prosecution. This provision is crucial for detecting illegal activities and ensuring that institutions fulfill their responsibility to prevent financial crimes.

4) Record Keeping and Retention of Records: The AML Act also mandates financial institutions and STO platforms to maintain records of all customer information, transactions, and financial records for a minimum of five years. These records must be made available to AMLO or other relevant authorities if requested for investigative purposes. According to record-keeping obligations under the AML Act, financial institutions must retain records that detail the nature, date, and amount of all financial transactions, including the identities of all involved parties (Transaction Details). The financial institutions must also keep the records of customer KYC and CDD information for a minimum of five years. This ensures that authorities can trace transactions and link them to legitimate or illicit sources (Customer Identification). Lastly, any Suspicious Transaction Reports ("STRs") filed by the financial institution must be kept for at least five years for potential future investigation.

5) Financial Intelligence Unit (FIU): The AMLO serves as Thailand's Financial Intelligence Unit (FIU), responsible for receiving, analyzing, and investigating suspicious financial transactions. AMLO plays a critical role in enforcing the AML Act and ensuring compliance by financial institutions, including STO platforms. AMLO has the authority to investigate suspicious activities and potential money laundering or terrorist financing schemes, freeze assets, or take legal action against entities suspected of being involved in illicit financial activities, and AMLO can cooperate with international regulators to trace illicit funds and combat cross-border financial crimes. Moreover, AMLO is also empowered to issue regulations and guidelines for institutions to follow, ensuring consistent compliance with AML/CFT standards.

6) The Role of Regulatory Authorities and Enforcement: In addition to AMLO, other regulatory bodies in Thailand play a role in ensuring compliance with AML and CFT laws. The Securities and Exchange Commission (SEC), for example, oversees digital asset businesses, including STO platforms, and ensures that they adhere to both securities regulations and AML standards. The Bank of Thailand (BOT) also plays a role in overseeing the financial system and enforcing AML measures in the banking sector. The enforcement of the AML Act is carried out through various channels. For example,

1. Regulators conduct regular inspections and audits of financial institutions to ensure compliance with AML laws.
2. Financial institutions that fail to comply with AML regulations will face fines, suspension of licenses, or criminal prosecution.
3. Thailand works closely and cooperates with global authorities or international regulators, such as the FATF and other FIUs, to share information and coordinate actions against illicit financial activities.

While Thailand has made significant progress in regulating STOs within the broader digital asset landscape, challenges remain in ensuring comprehensive AML compliance. One of the primary challenges is the decentralized nature of blockchain and STO platforms, which operate across borders and often without a central authority, making it difficult to track and monitor illicit activities. Additionally, emerging technologies such as decentralized finance (DeFi) and smart contracts may require further regulatory refinement to address potential gaps in compliance.

Key Provisions of Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing Act B.E.2559 (A.D.,2016) and its Amendments

The Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act B.E.2559 (A.D.,2016) (CFT Act) plays a crucial role in regulating and preventing the misuse of the financial system for terrorism financing and the proliferation of weapons of mass destruction. This legislation is especially relevant in the context of emerging technologies such as STOs and VASPs. These financial innovations, while providing new

opportunities for capital raising and investment, also pose potential risks in terms of being exploited for illicit purposes, including terrorism financing. This research examines the key provisions of the CFT Act as they apply to STOs in Thailand and evaluates their impact on preventing the misuse of digital assets and blockchain technology for unlawful financial activities, particularly terrorist financing and proliferation financing. The CFT Act is part of Thailand's commitment to international standards (e.g., the FATF recommendations), which focuses on preventing the flow of funds to terrorist organizations and entities involved in the proliferation of weapons of mass destruction and also outlines several key provisions that impact digital assets and STOs, ensuring that they do not become conduits for illegal financial activity.

1. Freezing and Seizing Assets Related to Terrorism and Proliferation Financing

The CFT Act grants authorities the power to freeze or seize assets linked to terrorism financing and the proliferation of weapons of mass destruction. In the part of STOs, this provision ensures that security tokens or other assets involved in illicit activities can be intercepted by authorities. If an STO platform or VASPs detects a transaction or customer linked to terrorism or the proliferation of weapons, they must report this activity to the relevant authorities, including the Anti-Money Laundering Office, and may be required to freeze or suspend the transaction until further investigation is conducted.

2. Monitoring and Reporting Suspicious Transactions

As part of the broader AML obligations, the CFT Act requires financial institutions and STO platforms to monitor for and report suspicious transactions that may be connected to terrorist financing or the proliferation of weapons of mass destruction. Key obligations under the CFT Act are as follows:

- **Suspicious Transaction Reporting:** Financial institutions, including STO platforms, are mandated to report any transaction that appears to be suspicious in nature. This could include unusual patterns of transactions, high-value transactions, or transactions involving high-risk countries.
- **Customer Due Diligence:** Financial institutions must conduct KYC procedures to verify the identities of their clients and assess the risk of terrorism financing or proliferation financing. If a customer is flagged as a politically exposed person ("PEP") or linked to known terrorist organizations, additional due diligence is required.

The reporting of suspicious transactions to AMLO ensures that illegal financial flows are detected, enabling authorities to prevent terrorism financing before it can be executed.

3. Prohibition of the Use of Financial Resources for Terrorist Financing

The CFT Act explicitly prohibits the use of financial resources, including digital assets, for terrorist financing and the proliferation of weapons of mass destruction. This provision is critical for STO platforms that facilitate the trading of security tokens. STO platforms must ensure that their systems do not facilitate or enable the flow of funds to individuals or organizations that are involved in terrorist activities or weapons proliferation. STO platforms are required to identify and verify their customers (KYC/CDD Compliance), ensuring that no terrorist group or individuals associated with the proliferation of weapons of mass destruction are able to use their platforms for illicit transactions. This also means that platforms must regularly update their risk assessments to identify new threats and mitigate the risks of misuse.

4. Cross-Border Financial Monitoring

The cross-border features of blockchain transactions represent significant challenges to the regulation of STOs. The CFT Act addresses this challenge by emphasizing the significance of international cooperation in the monitoring of the movement of illicit funds across borders. Thailand's cooperation with international bodies such as FATF and its Financial Intelligence Unit (FIU) allows for a global approach to terrorist financing prevention. Thailand also collaborates with international regulators to ensure that STO platforms are monitored globally and that suspicious activities are flagged for further investigation. This cooperation ensures that terrorist financing cannot occur simply due to jurisdictional differences.

5. Regulatory Oversight of Virtual Asset Service Providers (VASPs) and STO Platforms

The CFT Act mandates that STO platforms and other VASPs comply with rigorous AML/CFT regulations. These platforms are seen as critical points in the financial system where terrorist financing could be channeled, particularly given the anonymity and cross-border nature of digital asset transactions. STO platforms must register with Thailand's Securities and Exchange Commission (SEC) and comply with the SEC's guidelines on digital asset businesses (Registration and Licensing). They must also adhere to AML regulations, including the implementation of KYC, CDD, and Suspicious Transaction Reporting (STR) procedures to detect and report terrorism-related activities.

Impact of the AML and CFT Laws in Thailand on STOs

Thailand's AML and CFT laws are crucial for ensuring that the financial system is not exploited for illicit activities, including money laundering and terrorism financing. According to STOs and digital assets, these laws have significant implications in 3 parts as follows.

1. **Regulatory Oversight:** Issuers or investors in the STO platforms must comply with KYC and CDD requirements under the AML Act and CFT Act. This reduces the risk of money laundering and terrorist financing by ensuring that issuers or investors who are involved in STOs are accurately identified and the sources of their funds are verified.
2. **Transaction Monitoring:** Platforms that sell securities tokens are obligated to monitor and report suspicious transactions due to the borderless and anonymous nature of blockchain-based transactions. It shows that the platforms have the potential to be utilized to finance terrorism or fraud money.
3. **International Standards Compliance:** Thailand's legal framework is aligned with FATF standards, ensuring that STO platforms adhere to global AML/CFT practices. This alignment facilitates international cooperation and supports the country's efforts to prevent illicit financial activities.

LITERATURE REVIEW

The rise of blockchain-based financial instruments, particularly Security Token Offerings, has prompted increasing academic and regulatory attention toward the risks of financial crime in decentralized systems. This section reviews the relevant literature on the legal and compliance challenges posed by STOs, the roles of virtual asset service providers, and the global anti-money laundering frameworks developed to address emerging risks in the digital asset space.

Security Token Offerings and Their Legal Characterization

Security Token Offerings are a class of digital assets that represent ownership or rights in underlying financial instruments such as equity, debt, or revenue shares and are issued using blockchain technology. Unlike Initial Coin Offerings ("ICOs"), STOs are typically subject to securities laws and aim to provide more investor protection through regulatory compliance. The legal status of STOs varies by jurisdiction, based on whether the security token fulfills the definition of real-world security under national legislation (Minto, 2024). One of the most difficult issues in bringing such instruments into compliance with AML regulations has been their classification.

Virtual Asset Service Providers and Regulatory Risks

The FATF defines Virtual Asset Service Providers as entities that facilitate the exchange, transfer, safekeeping, or issuance of virtual assets on behalf of others. Virtual Asset Service Providers play a critical role in enabling STO transactions, but their operations—often pseudonymous and borderless—create significant vulnerabilities to money laundering and terrorist financing. According to Van Staden et al. (2025), one of the challenges is the lack of effective customer due diligence processes and regulatory inconsistencies among jurisdictions. These gaps increase the risk of regulatory arbitrage and weaken the international anti-money laundering framework. Moreover, to respond to the rapid evolution of the virtual asset landscape, the FATF has issued several updates to its 40 Recommendations, particularly Recommendation 15, which requires countries to ensure that VASPs are subject to AML/CFT obligations, including licensing, supervision, and enforcement. Furthermore, the necessity of efficient customer due diligence, recordkeeping, and reporting suspicious transactions is emphasized in Recommendations 10, 11, and 20. The FATF guidelines emphasize that countries must establish risk-based monitoring procedures in addition to enacting laws (FATF, 2023).

Challenges in Applying AML Standards to STOs

The application of conventional AML frameworks to STOs presents unique challenges. Minto (2024) notes that the inherent characteristics of blockchain (decentralization, immutability, and pseudonymity) can undermine traditional AML controls such as KYC verification and transaction tracing. Furthermore, decentralized finance protocols can function without recognizable intermediaries, hence challenging the enforcement of anti-money laundering legislation (Van Staden et al., 2025). These key challenges are especially concerning in places such as Thailand, where the regulatory structure is still evolving and may not adequately capture the intricacies of blockchain-based banking.

Existing Literature on AML and Virtual Assets in Thailand

While there is a growing body of research on global AML challenges in the crypto space, specific literature on Thailand's approach remains limited. Regulatory documents from the Thai Securities and Exchange Commission

(SEC Thailand, 2021) indicate preliminary steps in licensing and oversight, but academic studies suggest that Thailand’s current AML regime lacks comprehensive measures for dealing with STOs and related technologies. The literature highlights the absence of practical guidance for CDD, limited inter-agency cooperation, and a need for harmonization with FATF standards.

- **Digital Asset Regulation in Thailand:** Thailand began regulating digital assets in 2018 with the enactment of the Emergency Decree on Digital Asset Businesses B.E. 2561, which laid the foundation for controlling businesses dealing with digital assets, including digital exchanges and custodial wallet providers. By 2024-2025, Thailand implemented significant revisions and updates to its regulatory approach for Security Token Offerings, including clearer guidelines for various types of digital tokens, such as investment tokens, utility tokens, and real estate-backed tokens. These updates require issuers to seek approval from the Securities and Exchange Commission before conducting any offering, ensuring compliance with a structured, regulated environment.
- **Anti-Money Laundering (AML) and Customer Due Diligence:** In line with global trends, anti-money laundering efforts have intensified in Thailand, especially regarding digital asset service providers. Thailand’s AML laws, including the Anti-Money Laundering Act B.E. 2542 and the Securities and Exchange Act, impose obligations such as KYC and CDD processes. Although, the current framework continues to insufficiently integrate decentralized finance (DeFi) platforms and smart contract-based systems, resulting in enforcement inadequacies. The difficulty is in modifying these legal frameworks to effectively control decentralized operations, which frequently lack intermediaries.

Table 1: Comparative Analysis of FATF Recommendations vs. Thailand’s Legal Measures on AML for Security Token Offerings

Key FATF Recommendation	Core Requirement	Implementation in Thailand	Identified Gaps / Issues
Recommendation 10 Customer Due Diligence (CDD)	Identify and verify customers and beneficial owners	Implemented under Anti-Money Laundering Act B.E. 2542 and SEC regulations for digital asset businesses	No specific CDD requirements for decentralized STO platforms or cross-border investors
Recommendation 11 Record Keeping	Maintain records for 5 years	Included in Thai AML law and SEC’s licensing framework	Limited clarity on how blockchain-based STO records are to be preserved and accessed
Recommendation 15 New Technologies	Assess and mitigate ML/TF risks in digital assets and VASPs	Thailand has begun implementing licensing for digital asset exchanges and brokers	STOs not explicitly covered; DeFi platforms and smart contract-based issuers remain unregulated
Recommendation 20 Suspicious Transaction Reporting (STR)	Require timely reporting of suspicious transactions	STR obligations apply to financial institutions and licensed VASPs	Enforcement mechanisms for unlicensed STO facilitators are unclear
Recommendation 26-28 Supervision and Regulation	Supervise AML/CFT compliance of financial institutions and DNFBSs	SEC Thailand and AMLO coordinate supervision	Fragmented oversight for decentralized services and foreign-based issuers
Recommendation 40 International Cooperation	Effective cross-border information sharing	Thailand has legal provisions for cooperation and mutual legal assistance	Limited cooperation mechanisms tailored for cross-border STOs and blockchain transactions

Table 2: Comparative Analysis: Thailand vs. International Research Approaches on AML for STOs

Key Areas	Thailand’s Approach	International Research Insights (e.g., JMLC and FATF)	Observations/Recommendations
1. Legal Definition of STOs	No specific definition of STOs within primary legislation. Only general regulation of “digital assets” is in place.	Some countries (e.g., UK, USA) classify STOs as “securities” subject to securities laws (Van Staden et al., 2025).	Thailand should define and classify STOs clearly within its regulatory framework to ensure consistency in oversight and effective AML enforcement.

2. AML Compliance for VASPs	The SEC regulates certain digital asset service providers (VASPs), but DeFi and non-centralized platforms are not covered.	Internationally, regulations target both centralized and decentralized systems, including smart contracts and decentralized autonomous organizations (DAOs) (FATF, 2023; Minto, 2024).	Thailand should extend its AML obligations to decentralized platforms, smart contracts, and non-licensed providers, ensuring comprehensive oversight across all systems.
3. Customer Due Diligence (CDD)	CDD requirements are only for licensed entities under the SEC.	International research explores the use of e-KYC, biometrics, and AI to assess user behavior in DeFi platforms (Makkink et al., 2024).	Thailand should encourage the adoption of RegTech and explore digital solutions such as e-KYC and AI to enhance CDD, especially in decentralized systems.
4. Suspicious Transaction Reporting (STR)	VASPs must report suspicious transactions to the Anti-Money Laundering Office (AMLO), but DeFi and smart contract-based platforms are not explicitly addressed.	Research suggests the use of automatic suspicious pattern detection embedded in platforms for efficient STR reporting (Ochnio, 2024).	Thailand should create clear guidelines for identifying suspicious activities in STOs and consider automated systems for real-time reporting and monitoring.
5. Cross-Border Cooperation	Thailand has mutual legal assistance treaties (MLATs) for international cooperation, but blockchain-specific information exchange is underdeveloped.	Research in the EU recommends establishing a blockchain forensic network for cross-border cooperation, especially in tracking illicit activities across jurisdictions (Van Staden et al., 2025).	Thailand should enhance its international cooperation framework to address blockchain-specific cross-border risks, enabling better tracing of illicit transactions.
6. Supervision and Regulation	Regulatory supervision is primarily focused on licensed VASPs by the SEC and AMLO.	International standards call for comprehensive supervision mechanisms that include decentralized finance entities and cross-border cooperation (FATF, 2023).	Thailand should strengthen regulatory oversight to encompass decentralized systems and improve cooperation between regulators for more effective enforcement.

CONCLUSIONS AND IMPLICATIONS

Conclusions

This research has examined Thailand's current regulatory framework for anti-money laundering in the context of Security Token Offerings, comparing it with international standards, particularly those set by the FATF. The findings reveal that while Thailand has taken notable steps in regulating digital assets, significant gaps remain, especially in areas related to decentralized finance and smart contracts. These gaps prevent the country from fully mitigating risks related to money laundering and the financing of terrorism, as these new technologies introduce complexities that current regulations cannot fully address. The regulatory framework, while broadly in line with international standards, needs improvement in areas such as clear legal definitions for STOs, extended coverage for decentralized platforms, and better enforcement for blockchain-based systems. Although the FATF recommendations provide a global benchmark, Thailand's current approach does not yet fully capture the nuances of decentralized technologies.

Implications

The research reveals that while Thailand has taken important steps toward regulating Security Token Offerings under its anti-money laundering and counter-financing of terrorism framework, substantial gaps remain in its regulatory infrastructure. The implications of the findings are legal and policy-oriented, with broad consequences for regulatory reform, institutional coordination, investor protection, and international competitiveness.

1. *Implications for Legal and Regulatory Reform*

The current legal framework lacks sufficient clarity and adaptability to address the distinct nature of blockchain-based securities. Thailand's AML and securities laws—originally designed for traditional financial systems—do not adequately accommodate the decentralization, programmability, and cross-border

functionality of STOs (Securities and Exchange Commission, 2021). The lack of a specific regulatory framework for STOs results in legal ambiguity, which affects investor trust and blocks innovation in capital markets. In line with Supawich (2025), it is recommended that Thailand adopt a principle-based, technology-neutral legal framework that can evolve with digital innovation. The legal condition of tokens would be determined by their economic characteristics and risk profiles, rather than their form, in a framework that is beyond rigid definitions and incorporates functional regulation. This transition would support better compliance with FATF Recommendations 1 and 15, which promote a risk-based approach and specific AML measures for virtual assets and service providers (Financial Action Task Force [FATF], 2023).

2. *Implications for Regulatory Oversight and Coordination*

The regulatory supervision structure, which is fragmented and divided among the SEC, Anti-Money Laundering Officers, and other agencies, generates uncertainty for STO issuers and intermediaries (Thailand Anti-Money Laundering Office, 2021). This fragmentation has the potential to result in compliance burdens, regulatory arbitrage, and inconsistent enforcement. As Supawich (2025) highlights, the lack of a unified supervisory mechanism impedes effective monitoring of emerging risks in blockchain-based finance. To address this, Thailand should establish an integrated supervisory body or inter-agency task force focused specifically on digital assets and STOs. This would enable more coordinated AML/CFT supervision, facilitate information sharing, and reduce regulatory blind spots. It would also align with FATF's call for competent authorities to maintain clear oversight over virtual asset activities (FATF, 2023).

3. *Implications for Investor Protection and Market Integrity*

Investors in Security Token Offerings in Thailand are still in the early stages of getting legal protection. At this point, the legal system doesn't have clear rules about what information that token producers need to publish. Also, there aren't any clear ways to check events on the blockchain itself, and there aren't many legal options for fraud or bad management (Zohar, 2020). If these problems aren't solved, they could make issuers or investors less confident and adversely impact the country's reputation in global markets. To make the STO environment more trustworthy, officials need to make issuer responsibilities clearer, make sure that everyone can see how smart contracts work, and provide useful ways to settle disagreements. Also, platforms need to improve how they check users' identities and evaluate risks, especially when token sales happen across foreign lines. Moreover, Thailand must enhance due diligence obligations for STO platforms, especially regarding cross-border token offerings. Enhanced customer due diligence for high-risk transactions and ongoing monitoring is essential in mitigating the misuse of STOs for money laundering or terrorist financing (FATF, 2023; Minto, 2024).

4. *Implications for International Positioning*

Thailand's delay in updating its regulatory approach to match international standards—particularly those set by FATF and other advanced jurisdictions—could weaken its standing in the global digital finance space. As blockchain-based financial instruments gain traction worldwide, it becomes increasingly important for Thailand to show that its legal and regulatory systems are equipped to manage this shift (Van Staden et al., 2025). Without timely reform, the country risks not only missing out on new investment opportunities and slowing fintech development but also facing scrutiny in future international assessments on money laundering and terrorism financing. To stay competitive and credible, Thailand must pursue legal reforms alongside strong enforcement of AML measures.

Contribution/Originality: This research provides a valuable addition to the existing literature by summarizing the latest recommendations regarding money laundering for STO on the blockchain of the FATF and comparing it with the regulatory measures in Thailand. The findings highlight the significance of preventative measures for anti-money laundering on the blockchain, as well as the monitoring system of relevant officials or organizations that adhere to international guidelines. It advises relevant organizations or officials to consider findings alongside expert opinions, diverse analyses, and applicable regulations or relevant measures for an approach.

Funding: This research was funded by Research and Innovation Institute of Excellence, Walailak University, Thailand (Grant Number WU66237) and The APC was funded by Research and Innovation Institute of Excellence, Walailak University, Thailand (Contract Number WU66237).

Institutional Review Board Statement: The Ethical Committee in Human Research of Walailak University, Thailand has granted the approval of exemption for this research on 31 May 2024 (No. WUEC-24-206-01).

Conflicts of Interest: The funding sponsors did not participate in the study's design, data collection, analysis, interpretation, manuscript writing, and decision to publish the results.

Authors' Contributions: All authors contributed equally to the conception and design of the research. All authors have read and agreed to the published version of the manuscript.

REFERENCES

- Auer, R., & Weber, I. (2020). Banking on blockchain: A survey of the benefits, challenges, and regulatory issues of digital currencies and security tokens. *Journal of Financial Regulation and Compliance*, 28(4), 345–367. <https://doi.org/10.1108/JFRC-03-2020-0050>
- Baker McKenzie. (2025). *A complete guide to digital asset law in Thailand*. <https://www.bakermckenzie.com/>
- Chambers-Jones, C. (2017). *The Financial Crisis and Digital Currencies*. Palgrave Macmillan UK EBooks. https://doi.org/10.1057/978-1-137-47384-4_8
- Digital Asset Tokenization: A Game-Changer for Businesses and Investors Digital Asset Tokenization: A Game-Changer for Businesses and Investor. <https://gohawaii.us.com/digital-asset-tokenization-a-game-changer-for-businesses-and-investors/>
- European Securities and Markets Authority (ESMA). (2021). *Report on the application of EU law to blockchain and distributed ledger technology (DLT) in the securities markets*. <https://www.esma.europa.eu/>
- Financial Action Task Force (FATF). (2014). *Virtual currencies: Key definitions and potential AML/CFT risks*. OECD.
- Financial Action Task Force (FATF). (2020). *Red flag indicators for virtual assets*. <https://www.fatf-gafi.org/>
- Financial Action Task Force (FATF). (2023). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers (VASPs)*. <https://www.fatf-gafi.org/>
- Financial Action Task Force (FATF). (2024). *Money laundering national risk assessment guidance*. <https://www.fatf-gafi.org/en/publications/MethodsandTrends/Money-Laundering-National-Risk-Assessment-Guidance.html>
- Ganne, E. (2020). The rise of security token offerings: How blockchain and tokenized assets are transforming financial markets. *Global Blockchain Review*, 11(3), 52–75. <https://doi.org/10.1108/GBR-03-2020-0011>
- Makkink, I. M., Steyn, B., & Bezuidenhout, H. C. (2024). The role of freight forwarding companies in detecting and investigating trade-based money laundering. *Journal of Money Laundering Control*, 27(7), 26–42. <https://doi.org/10.1108/JMLC-04-2024-0069>
- Mehndiratta Kappal, J., Parashar, N., Mujumdar, M., Sharma, R., & Nair, P. G. (2025). An empirical study on the acceptance of CBDC by Indian bankers: A structural equation modelling approach. *Asian Economic and Financial Review*, 15(4), 630–647. <https://doi.org/10.55493/5002.v15i4.5382>
- Minto, A. (2024). Banks' internal governance obligations vis-à-vis money laundering risks emerging from the new technology-enabled means to transfer funds or value ("crypto assets"). *Journal of Money Laundering Control*, 27(7), 43–59. <https://doi.org/10.1108/JMLC-04-2024-0068>
- Minto, A. (2024). A regulatory approach to security token offerings and the future of capital markets. *Journal of Securities Regulation and Law*, 32(1), 12–34. <https://doi.org/10.2139/ssrn.3452317>
- Mokone, P. P. (2025). An analysis of the challenges in combatting money laundering within bureaux de change establishments in Botswana. *Journal of Money Laundering Control*, 28(7), 1–15. <https://doi.org/10.1108/JMLC-06-2024-0100>
- Ochnio, A. H. (2024). Recent developments in EU anti-corruption strategy: The missing element of the return of corrupt assets to "victim countries". *Journal of Money Laundering Control*, 27(7), 1–12. <https://doi.org/10.1108/JMLC-11-2023-0176>
- Securities and Exchange Commission (SEC), Thailand. (2021). *Guidelines on digital asset offerings*. <https://www.sec.or.th>
- Securities and Exchange Commission (SEC), U.S. (2019). *Framework for "investment contract" analysis of digital assets*. <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>
- Siregar, A., Murwaningsari, E., & Arsajah, R. J. (2025). The determinants of anti-corruption disclosure: Research on the Indonesia Stock Exchange. *Asian Economic and Financial Review*, 15(3), 467–486. <https://doi.org/10.55493/5002.v15i3.5349>
- Supawich, P. (2025). *Digital securities and blockchain technology: Legal perspectives on Thailand's capital market reform* [Undergraduate thesis, Chulalongkorn University].
- Thailand Anti-Money Laundering Office (AMLO). (2019). *FATF recommendations: International standards on combating money laundering and the financing of terrorism & proliferation*. Bangkok: AMLO.
- Thailand Anti-Money Laundering Office (AMLO). (2021). *Annual report on anti-money laundering and counter-financing of terrorism*. <https://www.amlo.go.th>
- Tran, Q. B., Nguyen, T. B. T., Nguyen, T. T. C., & Duong, D. A. (2024). Impact of perceived safety on customers' use of digital banking services at commercial banks: A case study in Vietnam. *Asian Economic and Financial Review*, 14(10), 782–797. <https://doi.org/10.55493/5002.v14i10.5225>
- United Nations. (2004). *United Nations Convention against Transnational Organized Crime*. <https://www.unodc.org>
- Van Staden, N., Kilian, E., & McIntyre, J.-L. (2025). A comparative dive into virtual asset legislation in South Africa, Mauritius, Namibia and the UK. *Journal of Money Laundering Control*, 28(7), 50–64. <https://doi.org/10.1108/JMLC-10-2024-0170>

- Van Staden, N., et al. (2025). Combatting AML risks in decentralized asset platforms. *Journal of Money Laundering Control*, 28(1), 32–45. <https://doi.org/10.1108/JMLC-04-2024-0069>
- Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21(1), 7–31. <https://doi.org/10.1093/rof/rfw068>
- Zohar, A. (2020). Blockchain technology and financial regulation: A global overview. *Journal of Financial Regulation and Compliance*, 28(2), 210–230. <https://doi.org/10.1108/JFRC-11-2019-0141>