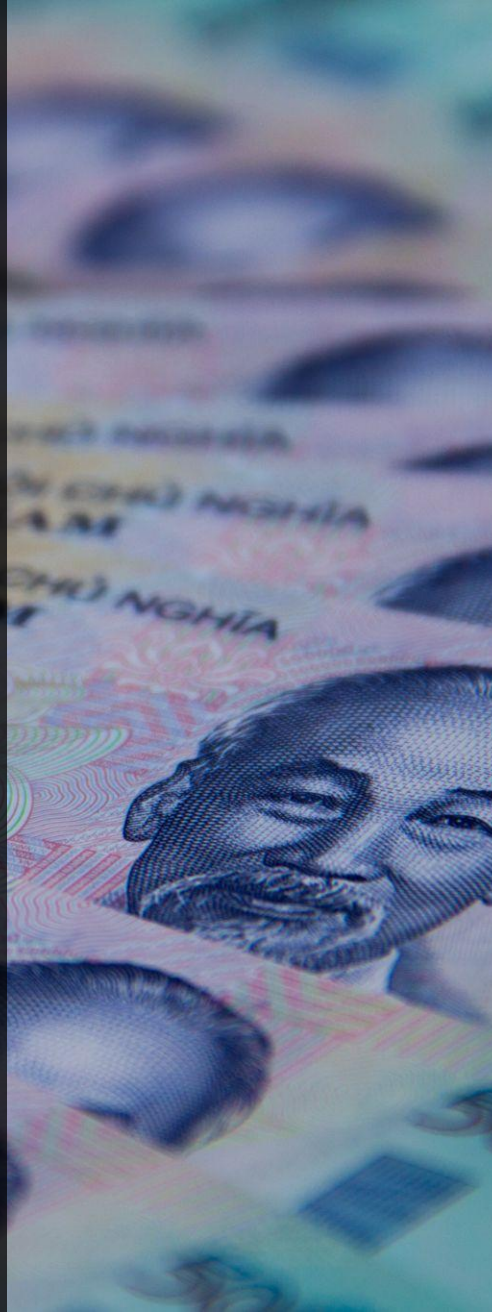


The New AML Law 2022

At a glance

May 2023

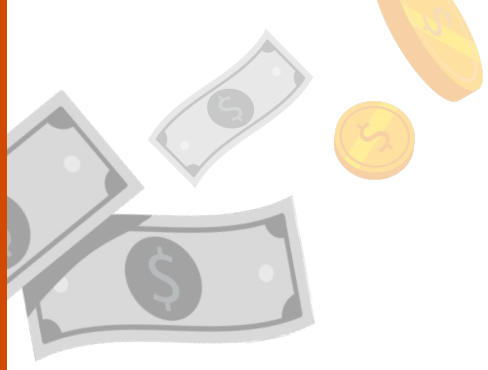
The new AML Law came into effect on 1 March, 2023. Reporting entities should seize the opportunity to establish their own internal regulations and capabilities, align with Vietnam Regulators, and contribute to preventing, mitigating, and combating financial crimes.

Background

- The State Bank of Vietnam (SBV) has announced a new Law on Anti-Money Laundering ("AML Law") that is in effect since March 1st, 2023. This AML Law is designed to address several shortcomings identified in the current AML Law from 2012 and align with international AML standards that Vietnam is required to implement.
- The main goal of this new Law is to improve the effectiveness of money laundering prevention activities and crime prevention in general. This also focuses on strengthening international cooperation to keep Vietnam's financial system safe and secure for everyone. By enhancing these measures, the new Law aims to create a more transparent and trustworthy financial environment in Vietnam.

What's new?

The changes that are brought by the new AML Law are important for all reporting entities to upgrade their procedures / processes and implement to help meet the compliance requirements set by the State Bank of Vietnam (SBV). Here are key highlights that reporting entities should start paying attention to:

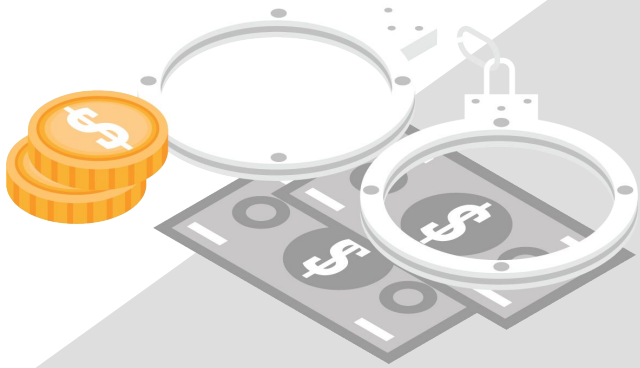


1 The scope of reporting entities that have obligations to the AML Law

- The organisations who provide payment intermediary services such as digital wallet services, collection and payment services are officially covered in the new Law. In addition, the new Law also clarifies the contents of specific industry sectors that are also covered by the AML Law, such as the securities, insurance, real estates, prize-awarding game / gaming and casino business, legal arrangement.
- The Government is authorised to stipulate the new industry that has high risk of money laundering.

2 Money laundering Risk Assessment and Client Risk Classification

- The reporting entities are required to conduct a thorough risk assessment and develop a money laundering risk management procedure that must include rules for customer classification by the low, medium, and high risk level and relevant measures that would apply according to the customer's level of risk.
- The SBV's Governor is authorised to provide the criteria and the method to perform the money laundering risk assessment of the reporting entities.



What's new?

3 Know Your Customer

- The new Law broadens types of customers of which the reporting entities must conduct KYC analysis, and further clarifies the scope of required KYC information for each type of customer. The requirement of "nature of the business relationship of the customer with the reporting entity" is added along with the current requirement of "purposes to set-up the business relationship with the reporting entity" as stipulated amongst the KYC information.

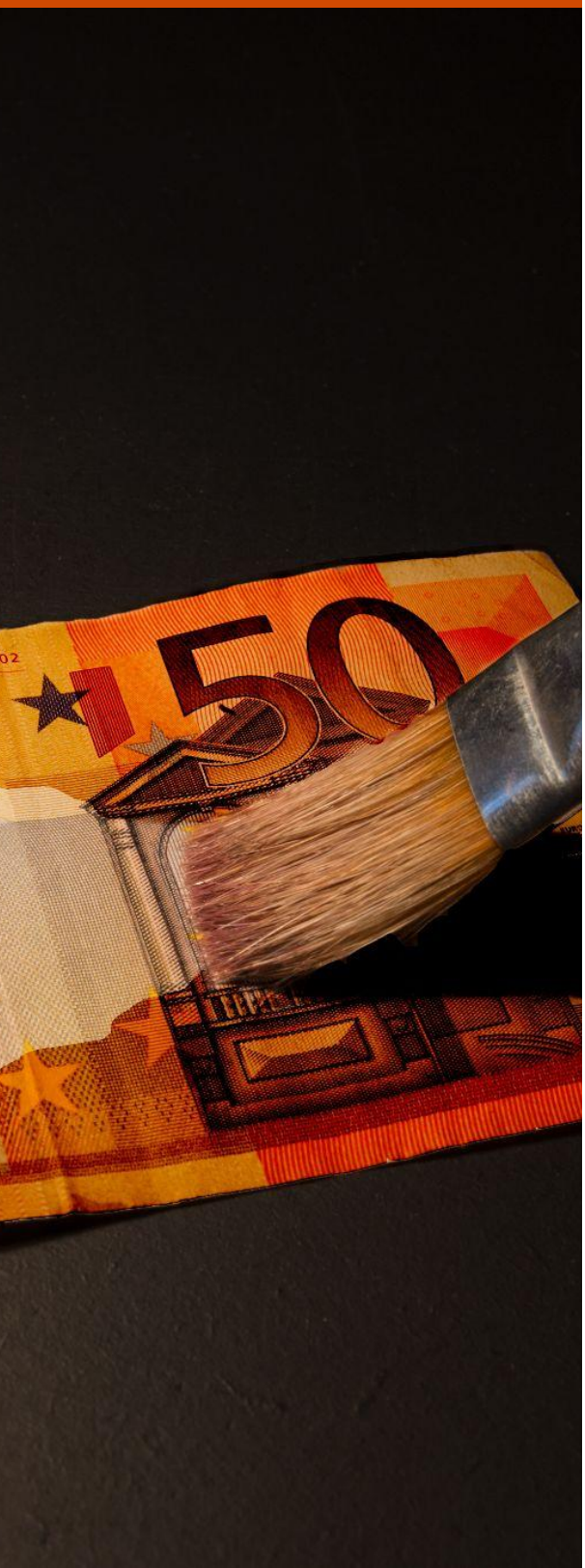
4 Foreign Politically Exposed Person (PEP)

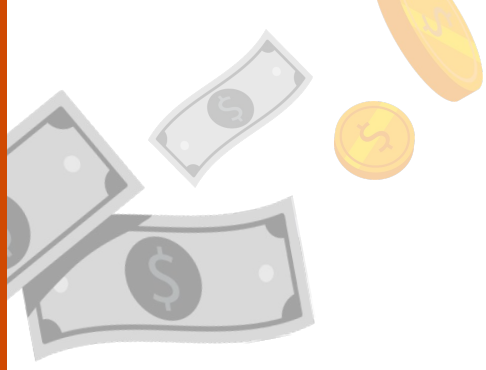
- The scope of foreign PEPs is broadened to include the foreign individuals with political influence who hold senior positions in international organisations, in addition to the senior positions in the organizations and bodies of foreign countries.
- In terms of the AML controls, the reporting entities are requested to apply proper measures to verify the source of wealth of the customer and the beneficiary or beneficial owners as an individual foreign PEP and the foreign PEP's associated persons.
- The new Law is silent on domestic PEPs.

5 Third party service provider / outsource organisation

- The new Law has replaced the term "business operation through introduction" by the term "third parties" or "the outsourced organisation" who handles the customer information verification and the customer due diligence activities on behalf of the reporting entity, and accordingly sets forth several conditions that the third party must satisfy.
- The new Law continues to emphasize the accountability of the reporting entities for the results of customer information verification and the customer due diligence by the third party, and in addition, must ensure the third party maintains confidentiality obligations.

What's new?



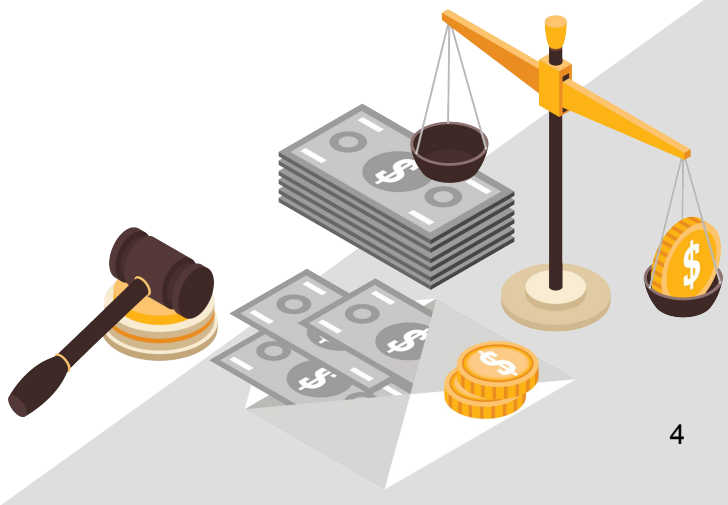


6 Transparency of the Information of Legal Arrangement

- When performing due diligence on a customer as a Trustee, the reporting entity may request the Trustee to provide the identity information of the Settlor / Grantor, the Trustee, the Beneficiary, and other parties concerned (if any), the natural person(s) who exercise the ultimate control(s) over the Trust.

7 Correspondent Banking Relationship

- When customers of the respondent bank are permitted to pay through the accounts that the respondent bank opens at the reporting entity, the reporting entity must ensure that the respondent bank has performed the required due diligence on these customers and is able to provide the respondent bank with the customer identification information upon the reporting entity's request.



What's new?

8 Suspicious Transaction Reporting (STR) and temporary measure

- The new Law sets out a list of suspicious signs for various sectors including banking, payment intermediary, life insurance, securities, prize-awarding game / gaming and casino businesses, and real estate business sectors.
- The new Law also clarifies the elements of suspicious transactions that are subject to the regulatory reporting, including the case upon learning / having reasonable grounds that the transaction is conducted at the request of the accused, the defendant, or the convicted person, and that the assets in the transaction belong to the accused, the defendant, or the convicted person, and that the related parties involved in the transactions are on the blacklist. Accordingly, the reporting entity must apply the postponement on the suspicious transactions as described above.
- The time limit for applying the transaction postponement measure shall not be more than 03 working days from the commencement date. The reporting entity shall be excluded from the legal liability for any consequence following application of a transaction postponement measure as stipulated.

9 Time limit for reporting

The new Law has made several changes to the time limit for reporting, in particular:

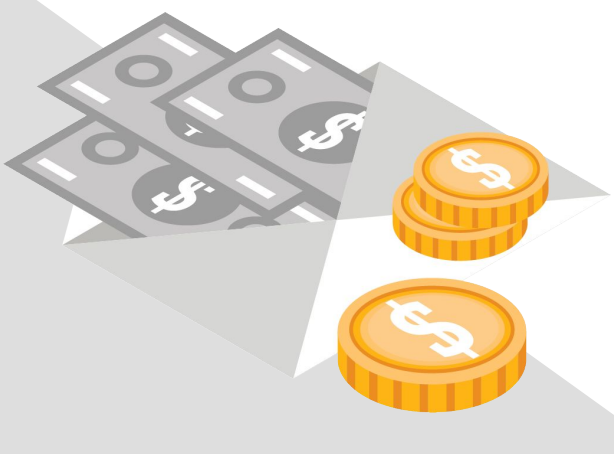
- Reporting the high value transactions and electronic money transfers will be within one working day from the transaction date for e-reporting and two working days from the transaction date for paper reporting.
- Reporting the suspicious transactions will be within three working days from the transaction or within one working day from the date on which the suspicious transaction is detected.
- Where the reporting entity detects that the suspicious transaction requested by the customer is indicating criminal activities, the reporting entity must report to relevant authorities and the SBV within 24 hours from the date of such detection.

What do firms need to do?

Here are some practical solutions to firms to consider in implementing the new AML Law:

Robust governance, culture, policy and procedure

- Strong oversight from the top management, a clear duty segregation and collaboration mechanism should be established across 3 LOD.
- An enterprise risk assessment guideline on ML, TF and sanction needs to be in place, executed periodically and upon material changes in the firm's business environment. This helps the firm fully be aware of threats and vulnerabilities and have proper actions to manage and mitigate.
- Staff should be fully aware of requirements in the new AML Law and implications to the firm from the business, risk and compliance perspective, periodically trained and updated on the risk landscape, and the firm's actions in managing and mitigating the ML, TF and Sanction risks.



Effective management reporting framework

This will provide the senior management with timely and actionable information, allowing them to perform effective oversight, as well as assist in promoting a robust AML/CFT culture across the organization and ensure the AML/CFT framework is not "set and forget" processes.

Effective implementation of the AML technology system

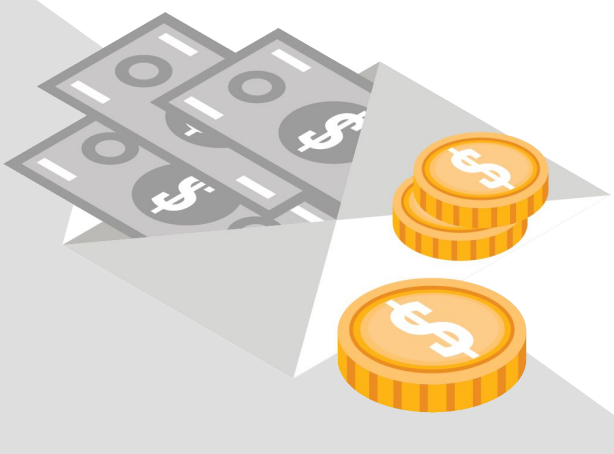
- Conformity to the data requirements structure(s) will ensure a solid foundation for scenario functionality, user interface display and overall application functionality.
- Data accuracy and completeness is crucial to ensure there is an effective AML technology system.
- This should also include the interaction with upstream and downstream applications such as core banking platforms, case management systems as well as management information systems.
- Sufficient resources with required skills and experience to conduct effective assessments and refinements of the system are also very essential for the successful implementation of the AML technology system.

What do firms need to do?

Here are some practical solutions to firms to consider in implementing the new AML Law:

Effective investigation

- The firm should ensure staff involved in handling suspicious transaction alerts generated by the transaction monitoring system are adequately skilled and experienced to identify and assess criminal activity, and make appropriate decisions for escalation or reporting.
- A list of minimum standards when investigating an alert should be established. This will help to maintain the quality and accuracy of the investigations. Using a well designed, calibrated and risk based transaction monitoring (TM) system will permit the investigators to focus on the specific TM scenarios that triggered the risk alerts.



Effective outsourcing programme

Good governance and strong oversight of any outsourced function is established. This is to ensure the outsourced service provider (OSP) performs the services to the standards required by the firm's internal regulations and in compliance with the local regulations on the AML/CFT and proliferation of weapons of mass destruction. Implementing the outsourcing programme in this space effectively can free up and enable the highly skilled and experienced financial crime risk and compliance resources of the firm to focus on higher risk transactions and activities.

Effective Quality Assurance (QA) programme

- An effective QA programme should be risk focused, varying the frequency and intensity of monitoring to the level of risk identified.
- In terms of the governance and operating model for the QA programme, this should be sufficiently independent, having appropriate reporting lines to escalate the issues / weaknesses identified across the enterprise wide AML/CFT framework to the senior management.
- A matured QA loop would also promote the desired AML/CFT mind-set and ethical standards amongst the firm's employees.

Contact us

Ms. Dinh Hong Hanh

Partner, Financial Services Leader
PricewaterhouseCoopers Consulting (Vietnam) Ltd
dinh.hong.hanh@pwc.com

Mr. Hiran Cabraal

Director, Financial Crime Risk Consulting Service
PricewaterhouseCoopers Consulting (Vietnam) Ltd
cabraal.hiran@pwc.com

Ms. Vo Tan Bich Ngoc, CAMS

Senior Manager, Financial Crime Risk Consulting Service
PricewaterhouseCoopers Consulting (Vietnam) Ltd
vo.tan.bich.ngoc@pwc.com

Ms. **Hoang Thi Quynh Phuong**

Senior Manager, Financial Crime Risk Consulting Service
PricewaterhouseCoopers Consulting (Vietnam) Ltd
hoang.thi.quynh.phuong@pwc.com

PwC Vietnam Offices

Ho Chi Minh

8th Floor, Saigon Tower
29 Le Duan Street, District 1,
Ho Chi Minh City, Viet Nam
T: +84 28 3823 0796

Ha Noi

16th Floor Keangnam Landmark 72
Pham Hung Road, Nam Tu Liem District,
Hanoi, Viet Nam
T: +84 24 3946 2246