Combatting money laundering and terrorism financing

The role of Malaysia's digital banks

The five companies in Malaysia that will eventually be awarded the coveted digital banking licence by Bank Negara Malaysia (BNM) would have proven their superiority above the crowd of applicants. But until that announcement is made in the first quarter of 2022, the race to be Malaysia's first digital banks remains hot.

It's clear from BNM's Policy Document on Licensing Framework for Digital Banks that there are great expectations placed on the shoulders of the country's digital banks. Above the directive to service the unserved and underserved segments of the community, digital banks will be required to join in the nationwide commitment on anti-money laundering and counter financing of terrorism (AML/CFT).

Hence, applicants of the digital banking licences would do well to showcase their capabilities in complying with AML/CFT requirements at this early stage – if only to reassure BNM that they have a clear understanding of the AML/CFT laws and regulations and share BNM's commitment to this purpose.

Where to start?

Applicants should first identify and assess the potential money laundering and terrorism financing (ML/TF) risks posed by their intended customer base and business offerings. Hard-hitting questions need to be asked, such as:

- What is my level of exposure to ML/TF risks if I allow accounts to be opened through agents?
- What is the likelihood that scammers or "money mules" will open a digital bank account?
- How might the transaction channels I am offering be misused for ML/TF?

These pulse checks will help to identify the control measures needed to mitigate such risks and allow digital banks to set their risk appetite.

It does not stop there. Applicants should thereafter outline the AML/CFT compliance programme to be implemented should they successfully receive a digital banking licence. Here, applicants need to prove they can and will mitigate the ML/TF risks identified and comply with regulatory requirements. This includes but is not limited to:

- determining the governance and oversight functions as well as resources;
- drafting policies and procedures;

- developing plans to identify customers such as via electronic-know-your-customer (e-KYC); and
- identifying user and system requirements for transaction monitoring and name screening systems.

The outline of the applicant's AML/CFT compliance programme should be part of their proposal to BNM as an assurance that they have a thorough action plan in place.

Addressing the challenges

It bears repeating that digital banks are likely to face different levels of challenges compared to traditional financial institutions, and this also applies to mitigating ML/TF risks.

By the nature of its set-up, digital banks lack the need for a face-to-face interaction with its customers, thereby adding another layer of risk in verifying that the customers are who they say they are. In today's digital age where documents can be forged, a thorough study needs to be done to determine how customer due diligence exercises can be completed at a level that can be accepted satisfactorily.

To add to that challenge, regulatory guidance are principle-based and leading practices in the digital banking space are still in their inception stage thus posing a limitation for industry players to develop and benchmark their AML/CFT compliance programmes.

The complexity of managing ML/TF risks is further exacerbated when we take into account the cyber threat landscape that continues to evolve as more sophisticated technology tools and solution become readily available to individuals with malicious intent. Digital banks should ensure they have the capability, either by hiring specialised talents or engaging industry experts, to assist with interpreting the regulatory requirements, assess the applicants' potential ML/TF risks and work with them to outline a high-level compliance programme.

The long-haul factor

Successful applicants of BNM's digital banking licence will have to undergo an operational readiness review. In this phase, licensed digital banks should see themselves getting ready to implement AML/CFT compliance programme, such as obtaining its Board approval for the AML/CFT policies and procedures, procuring solutions for transaction monitoring as well as name screening that fits the bank's business needs and requirements, developing and launching digital customer identification measures (such as biometric, facial recognition, document fraud detection, optical character recognition), plus a whole gamut of stringent regulatory requirements.

This is a crucial phase to get right from the get-go as licensed digital banks need to submit to the central bank an independent external assurance to demonstrate they are able to steer through the storm of ML/TF risks before they can commence their growth journey. This need not be viewed as an audit, but rather an opportunity to work with industry experts to identify the right measures to meet foreseeable risks and early detection of possible control gaps.

With the business in operation, licensed digital banks will need to continuously enhance their AML/CFT measures. This includes periodic risk assessments and enhancement of the AML/CFT compliance programme lest they are subject to fines or have their licence revoked. Regulators across various countries including Malaysia have been ramping up enforcement actions against errant financial institutions, and we can expect the same stringent actions against digital banks.

Digital banks will be warmly welcomed for its potential to expand the coverage of much needed financial products and services to the masses. It must also be reminded that the links among banks, both traditional and digital, and banking stability are essentially anchored on public trust and confidence. Any significant disruption in banking operations will cause ripple effects across other banks and will affect society as a whole.

Hence, digital banks should be proactive in managing their AML/CFT compliance programme to combat ML/TF, and thereby add their weight behind BNM in securing banking stability within Malaysia. ■

Contact us

Yeoh Xin Yi
Head of Financial Risk Management and
Digital Banking Leader
KPMG in Malaysia

E : xinyiyeoh@kpmg.com.my

Khurram Pirzada
Executive Director
Forensic, AML & Sanctions
KPMG in Malaysia

E : khurrampirzada@kpmg.com.my

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

www.kpmg.com.my/digitalbanking