



LAWTECH
MALAYSIA

FINTECH WHITE PAPER 2020: e-KYC & DIGITAL BANKS

6TH FEBRUARY 2020



LAWTECH MALAYSIA

Authors

Jenna Huey Ching

Benjamin Hor

Designers

Cheah Si Winn

Jenny Low

Disclaimer

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. LTM accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Tech Law Sdn Bhd (LTM) is a company registered in Malaysia with registered number 1296585-T and its office at Level 3, East Wing, 5, Jalan Stesen Sentral, Kuala Lumpur Sentral, 50470 Kuala Lumpur, Federal Territory of Kuala Lumpur, Malaysia.

Please email us at info@lawtech.my for more information.



Table of Contents

01	FinTech
04	e-KYC
11	Digital Banks
18	Considerations for the Future
25	Featured Companies
32	Moving Forward
34	References
38	Contact us



LAWTECH
MALAYSIA

0
1

FinTech





What is FinTech?

Bank Negara Malaysia (“the Bank”) defines FinTech as **technological innovation that is to be utilised in the provision of financial services**¹. There are many variations of FinTech that exist. Both e-KYC and Digital Banks are categories of FinTech that operate in the industry. Other examples include cryptocurrency or digital assets, insurtech, equity crowdfunding, remittance, peer-to-peer financing and e-wallets.

250 FINTECH COMPANIES TRANSFORMING FINANCIAL SERVICES

WALLETS & MONEY TRANSFER



PROCESSING & PAYMENTS INFRASTRUCTURE



CAPITAL MARKETS & TRADING



CROWDFUNDING



REAL ESTATE INVESTING



BLOCKCHAIN



WEALTH MANAGEMENT



PERSONAL FINANCE & MOBILE BANKING



GENERAL LENDING & MARKETPLACES



PERSONAL & CONSUMER LENDING



BUSINESS LENDING



MORTGAGE LENDING



CREDIT SCORE & ANALYTICS



MERCHANT SERVICES



FINANCIAL SERVICES & INFRASTRUCTURE



REGULATORY & COMPLIANCE



INSURANCE



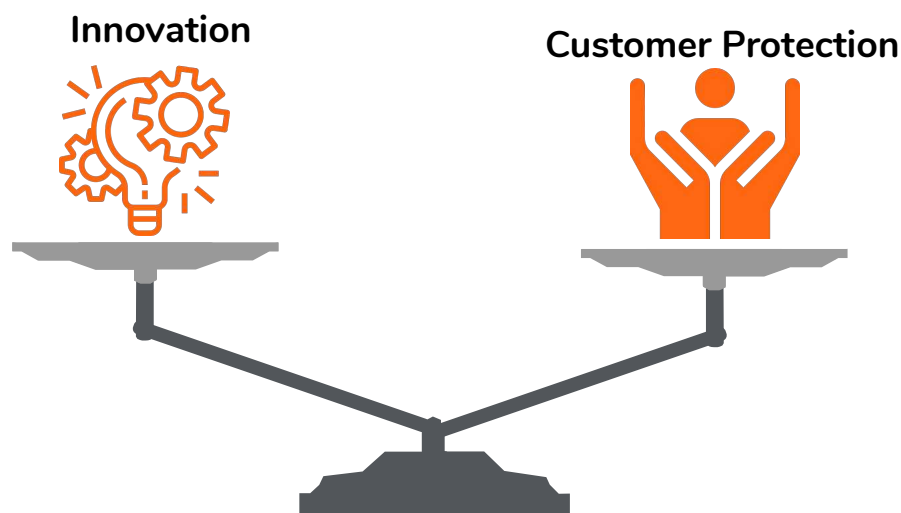
Source: CB Insights

1. Bank Negara Malaysia, *Financial Technology Regulatory Sandbox Framework* (BBNM/RH/PD 030-1, 18 October 2016)



How does FinTech link to Bank Negara Malaysia's Exposure Drafts on Electronic Know-Your-Customer (e-KYC)² and Digital Banks,³ both of which were recently published in December 2019?

With the rapid growth of FinTech, the impact on the financial industry (and by extension, the corporate world) is significant. **Overregulation, changing global business models and customer needs, and the advances of technology and innovation** have shaped the FinTech ecosystem into what it is today - to be an essential component in striking a **balance between innovation** in the finance industry and the **Bank's role in promoting monetary and financial stability**.



What is LTM's role in the FinTech scene?

The financial sector is a key industry to prepare for digital transformation - it is one of the **most heavily regulated industries** and is **one of the pillars of the digital ecosystem**. We believe that the **financial industry**, along with the **legal and regulatory industries** (collectively abbreviated as FLR), need to **converge and collaborate with one another**. LTM's mission is therefore to become a **platform that shares knowledge and facilitate policy-discussion by bringing industry experts together**.

Our **Fintech event: e-KYC and Digital Banks** held on **6 February 2020**, which consists of both a **private roundtable discussion**, and **public panel session** is a culmination of **collective effort within the industry to democratise knowledge and ultimately upscale the workforce**. With a **sold-out event of 200 pax**, our event attracted attendees across different industries which includes **lawyers, government officials, bankers, startups, compliance officers, corporate bodies, and even technical experts**. By bringing the industry together, we have also gathered some insights from the experts and compiled it into this White Paper.

2. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019)
3. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019)



e-KYC





What is e-KYC (electronic Know-Your-Customer)?

When a person seeks to create a bank account, the financial institution would need to verify his/her identity and assess his/her suitability in order to prevent fraud (otherwise known as the onboarding process). This is normally done through verification checks such as requesting for identification documents (e.g. utility bills and bank statements), which often require face-to-face interactions.

Identity Verification Options	Coverage	On-boarding Friction	Level of Security
Request user for identification documents e.g. bank statements, utility bills	Medium	Medium	Low
Substantiating customer information with an independent source e.g. contacting customer's employers	Medium	High	Medium
Substantiating customer information with an independent source e.g. through database maintained by relevant authorities	Medium	Low	Medium
Contacting customer through any digital communication channel to digitally verify customer's identity, e.g. eKYC	High	Low	Medium
Request customer to perform a credit transfer to another licensed person and ensure the customer details returned are consistent	Medium	High	High

Source: Jumio

On the other hand, e-KYC is the digitalisation of onboarding processes which leverages on newer technologies for verification and assessment. **The Bank defines e-KYC as a means to establish business relationships and conducting due diligence by way of electronic means, including both online and mobile channels.**⁴ This is usually carried out through biometrics (e.g. face, fingerprints) and liveness detection technologies. In other words, it is a modern approach for financial institutions to onboard new clients.

Why is e-KYC so attractive?⁵

Banks and financial services providers are striving to increase new customer acquisition through faster, easier and lower-cost digital channels. Yet, the **stringent e-KYC requirements and growing threat of online fraud and deepfakes** are taking a toll on the **cost of compliance and creates a layer of complexity**. On one hand, financial services companies need to ensure quick customer onboarding process while, on the other hand, to verify the identity of their online customers to fulfil regulatory requirements and prevent fraudulent activities.

Modern e-KYC, AML and identity verification technologies can transform many of the manual processes, particularly those related to meeting regulatory requests and gaining useful data insights to meet business objectives. Identity verification providers such as **Securemetric, Innov8tif, V-Key, and Jumio** provides solutions that leverage on advanced technologies including AI, face-based biometrics, machine learning and cybersecurity to fight identity fraud and deepfakes, maintain compliance and onboard good customers faster. If properly managed, **e-KYC solutions can improve efficiency and drive costs down to create a great user experience for users.**

4. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 5.2

5. Frederic Ho, VP of Jumio, APAC Region



Key Points on Bank Negara Malaysia's e-KYC Exposure Draft (issued on 16 December 2019)

Objectives of the e-KYC Exposure Draft⁶

1. To enable safe and secure application of e-KYC technology in the financial sector.
2. To facilitate the Bank's continued ability to carry out effective supervisory; oversight over financial institutions.
3. To ensure effective Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) control measures.

Who they apply to?⁷

1. Licensed banks;
2. Licensed investment banks;
3. Licensed Islamic banks;
4. Licensed life insurers;
5. Licensed family takaful operators;
6. Prescribed development financial institutions;
7. Licensed money-changing operators;
8. Licensed remittance service providers; and
9. Approved non-bank issuers of designated payment instruments and designated Islamic payment instruments.

Is prior approval required from Bank Negara to implement e-KYC?⁸

Only certain institutions require prior written approval which are:

1. Money-changing operators;
2. Licensed remittance service providers;
3. Approved non-bank issuers of designated payment instruments; or
4. Approved non-bank issuers of designated Islamic payment instruments.

6. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 5.2
7. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 5.2
8. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 10.1



What are the minimum requirements?

e-KYC implementation for each type of product or service would require the financial institution to:

1. **Obtain Board Approval.**⁹

However, Board Approval shall only be granted if the Board is able to ensure the effective implementation of appropriate policies and procedures to address any risks associated with the implementation of e-KYC. These include operational, information technology (IT) and money laundering and terrorism financing (ML/TL) risks.¹⁰

2. **Demonstrate continuously that their identification and verification of customers are effective.**¹¹

This would require an appropriate combination of authentication factors. Three main considerations were stated in the policy document include but not limited to:¹²

- a. utilise biometric technology to verify the customer against a government issued ID;
- b. utilise fraud detection technology to ensure that the government issued ID used to support e-KYC customer verification is authentic;
- c. utilise liveness detection technology to ensure the customer is a live subject and to detect impersonation attempts (e.g. use of photos, videos, facial masks); and
- d. Continuously identify and address potential vulnerabilities (e.g. exposures to IT, operational and ML/TF related risks).¹³

3. **This shall include conducting reviews on the e-KYC solution and, where applicable, submit periodical feedback to technology providers.**¹⁴

4. **Meet the minimum threshold for False Acceptance Rates (FAR) of less than 5% (only applicable if the e-KYC solution is automated with the use of artificial intelligence, machine learning or other forms of predictive algorithms, whether in whole or in part)**¹⁵

If FAR exceeds 5% for more than 3 consecutive months, the institution will be required to notify the Bank within 7 working days and provide:¹⁶

- a. An assessment of the current performance of the e-KYC (includes reasons for the FAR);
- b. Proposed action plan to reduce the FAR; and
- c. Proposed mitigating actions or additional controls (e.g. manual reviews) to safeguard the effectiveness of the e-KYC solution.

9. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.1
10. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.2
11. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.3
12. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.6
13. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.10
14. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.11
15. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.8
16. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) Appendix 1, para 3



5. Ensure safeguards are in place when there are limited data points to determine the accuracy of the e-KYC solution during the initial deployment stage.¹⁷ This automatically applies to setting up a current account and savings account.¹⁸

These safeguards include a complete combination of four (4) authenticating factors but not limited to:¹⁹

- a. utilise biometric technology to verify the customer against a government issued ID;
- b. utilise fraud detection technology to ensure that the government issued ID used to support e-KYC customer verification is authentic;
- c. utilise liveness detection technology to ensure the customer is a live subject and to detect impersonation attempts (e.g. use of photos, videos, facial masks); and
- d. require a customer to perform a credit transfer from the customer's existing bank account with another licensed person and ensure the customer details (e.g. name) returned on said transfer is consistent with the initial details supplied by the customer.

17. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.13

18. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) para 7.3

19. Bank Negara Malaysia, *Electronic Know-Your-Customer (e-KYC) Exposure Draft* (BNM/RH/ED 030-2, 16 December 2019) Appendix 2, para 1

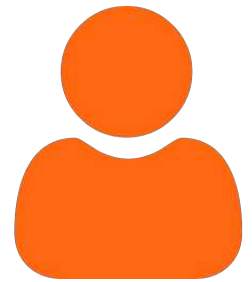


Key Comments on Bank Negara Malaysia's e-KYC Exposure Draft (issued on 16 December 2019)

Director's obligations are too onerous - One industry expert

The Board generally serves as the overseeing body of a company. Requiring the Board to approve e-KYC implementation for each type of financial product or service would increase the frequency of board meetings and drive up costs because of the need to approve projects that concern e-KYC related technologies/innovation.

The education process for board-level executives will also be burdensome because they have to be involved in the implementation stage when they should only be concerned with oversight. e-KYC is only the first level of many technology-driven areas which require industry expertise. Transaction monitoring is next. In short, directors will need to know end-to-end implementation. Such onerous obligations may stifle innovation and progress due to cumbersome process and onerous obligations on the Board



Industrial Expert

There needs to be greater emphasis on tamper-proofing requirements and additional checks for those in grey areas- Er Chiang Kai, CTO of V-Key

7.6 and Appendix 2.2 should include utilise tamper-proofing technology to ensure that the software used for e-KYC is not tampered with and that the integrity of the result is assured when received by the back-end server. A financial institution should also be required to conduct additional checks on customers who may not have reached a positive identification threshold through the standard checks, but have also not been rejected yet.

Ubiquity needs to encouraged as far as possible - Er Chiang Kai, CTO of V-KEY

Android and Apple may be the most popular softwares but they are not the only ones. The existence of different software updates, versions (e.g. jailbroken), and phone models create a convoluted ecosystem for e-KYC solutions to function seamlessly. As far as possible, a financial institution should minimise the use of special device features so that the use of e-KYC can be ubiquitous.



*Er Chiang Kai,
CTO of V-KEY*



*Chris Leong,
Softspace*

e-KYB has not even been addressed yet - Chris Leong, Softspace

e-KYB (electronic Know-Your-Business) is an extension KYC which is the practice of verifying a business. Some examples of verification include registration credentials and identifying the ultimate beneficial owner(s). The key difference between the two are the entities - KYB applies only to businesses whereas KYC applies customers (individuals) of businesses. e-KYB needs to be addressed as global regulations becomes more stringent.

The e-KYC Exposure Draft does not address the industry's ability to verify biometrics which would affect Digital Banks - Chris Leong, Director of Strategy, Softspace

There are currently no publicly available APIs or SDKs for biometric checks for the Malaysian landscape which makes it impossible to implement a biometric system for verification/onboarding. Digital banks, which would require such data, also become impossible.

There needs to be defined thresholds for e-KYC solutions - Tien Soon, COO of Innov8tif

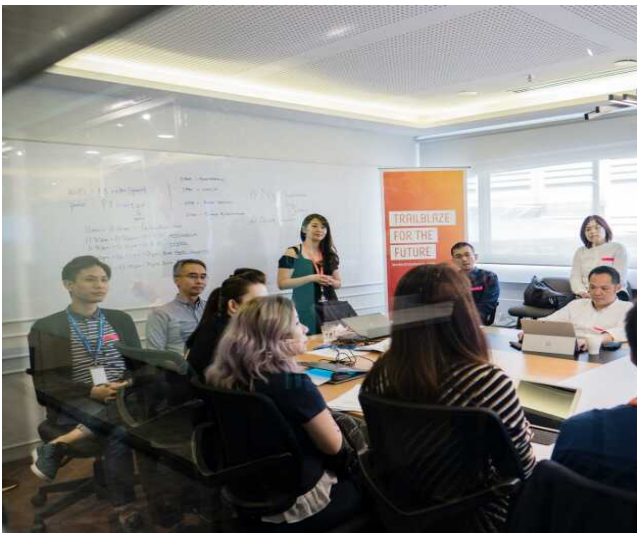
e-Wallets appear to be a strong precedent where the treatment of Money-Service-Businesses (MSB) in terms of risk appetite are similar across different MSBs - they have similar monthly-transaction slices and monitoring controls. The Bank should be clearer on what they are willing to accept as an e-KYC solution by defining the acceptance threshold for each solution.



*Tien Soon,
COO of Innov8tif*



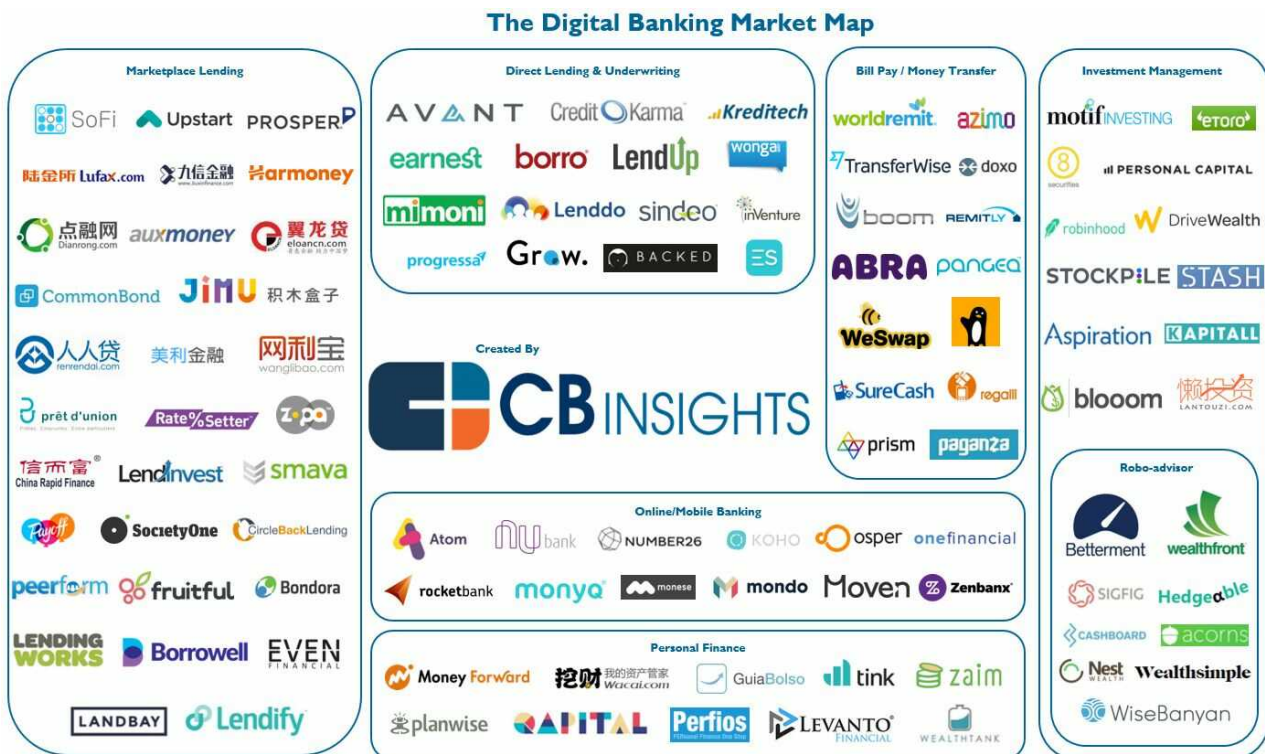
Digital Banks





What are Digital Banks?²⁰

A digital bank (also known as a neo/challenger bank) is essentially a bank that does not have a physical presence as services are provided online. Digital banking is the digitisation (or moving online) of all the traditional banking activities and programs services that were historically were only available to customers when they are physically inside of a bank branch. This includes activities like money deposits, withdrawals and transfers, and applying for new accounts. Some examples of digital banks include Monzo, Number26, Starling, Fidor, and Atom.



Source: CB Insights

Why are Digital Banks so attractive?²¹

Digital banks offer simplified application processes, great user experiences, diversified financial products fit for different lifestyles and financial needs and ease of management. They are often more efficient, allowing new processes and products to be integrated with their systems. Customers are able to connect easily which opens up new forms of financial interactions that are convenient, such as opening bank accounts online and accessing third-party products. This allows many digital banks to acquire customers on a large scale by serving underserved segments that do not have easy access to financial services. Some examples include SMEs and rural areas which do not have a bank branch. Interestingly, the Bank has stated that they only intend to issue five (5) digital bank licences²² which raises questions as to whether there would be a balance between existing banks who would conduct joint ventures and new players to secure the license.

20. Anatoly V Zhuplev, *Disruptive Technologies for Business Development and Strategic Advantage* (IGI Global, 22 June 2018)

21. Antony Jenkins, 'The demise of the traditional banking model is actually good news for all of us' (*Quartz*, 27 November 2019) <<https://qz.com/1755889/the-democratic-benefits-of-digital-banking/>> accessed 8 February 2019

22. Bank Negara Malaysia, 'Exposure Draft on Licensing Framework for Digital Banks: Press Release' (27 December 2019) <https://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4970> accessed 9 February 2020



Key Points on Bank Negara's Licensing Framework for Digital Banks Exposure Draft (issued 27 December 2019)²³

24

Who does this apply to?

1. Applicants applying for a licence under section 10 of the Financial Services Act 2013 ('FSA') or section 10 of the Islamic Financial Services Act 2013 ('IFSA');
2. Licensed digital banks as defined under section 10 of the FSA and section 10 of the IFSA; or
3. Shareholders who require an approval under section 90 of the FSA or section 102 of the IFSA for the holding of interest in the shares of the proposed licensed digital bank.

25

Objectives of the Licensing Framework for Digital Bank Exposure Draft

1. To enable admission of digital banks with strong value propositions whilst **safeguarding the integrity and stability of the financial system as well as depositors' interests**.
2. To offer banking products and services to underserved or unserved market primarily through digital or electronic means.
3. To expand meaningful access to and responsible usage of suitable and affordable financial solutions for the underserved and unserved market.
4. To further elaborate on the eligibility requirement and application procedures that must be complied with by an applicant intending to carry on digital banking business or Islamic digital banking business.
5. To implement a 'foundational phase' as defined in paragraph 1.4 of the Licensing Framework for Digital Banks: Exposure Draft.
6. To explain the business limitations and regulatory framework applicable during the foundational phase.
7. To explain the business activities that must be undertaken and the physical access points that may be established by the licensed digital bank.

23. Do take note that there are other policy documents that have been issued by the Bank to supplement this exposure draft which are Bank Negara Malaysia, *Application Procedures for Acquisition of Interest in Shares and to be a Financial Holding Company* (BNM/RH/PD 030-5, 27 December 2019) and Bank Negara Malaysia, *Application Procedures for New Licences under Financial Services Act 2013 and Islamic Financial Services Act 2013* (BNM/RH/PD 030-4, 27 December 2019)

24. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 2.1.

25. Objectives were derived from the overarching principles contained in both the Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) and Bank Negara Malaysia, 'Exposure Draft on Licensing Framework for Digital Banks: Press Release' (27 December 2019) <https://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4970> accessed 9 February 2020



What are the factors for consideration in assessing the best interest of Malaysia criteria?

1. Applicants' commitment in sustainably driving **financial inclusion to undeserved and hard-to-reach segments that may be unserved**, which includes retail as well as micro, small and medium enterprises (MSMEs), without jeopardising the interest of depositors.
2. Ability of shareholders of a licensed digital bank to offer an enforceable undertaking pursuant to section 259 of the FSA or section 270 of the IFSA.

27

What about existing licensed banks and Islamic banks?

Licensed banks and licensed Islamic banks may apply for a digital bank licence separate from their current licensed entity should they wish to carry on digital banking business or Islamic digital banking business in a joint venture with other parties.

However, this does not preclude licensed banks and licensed Islamic banks from digitalising their current business operations, which remains within the scope of their existing banking licence and **does not require the application of a separate digital bank licence**.

28

What about investment digital banks?

An applicant for a licence to carry on investment banking business must simultaneously apply to Securities Commission Malaysia for a CMSL (Capital Markets Services Licence) to conduct regulated activities under the CMSA. (Capital Markets and Services Act 2007).

29

What criteria must I fulfil whilst operating during the foundational phase?

1. Maintain at all times a minimum amount of capital funds of RM100 million.
2. Ensure that the total size of assets do not at all times exceed the limit of RM2 billion during the foundational phase.

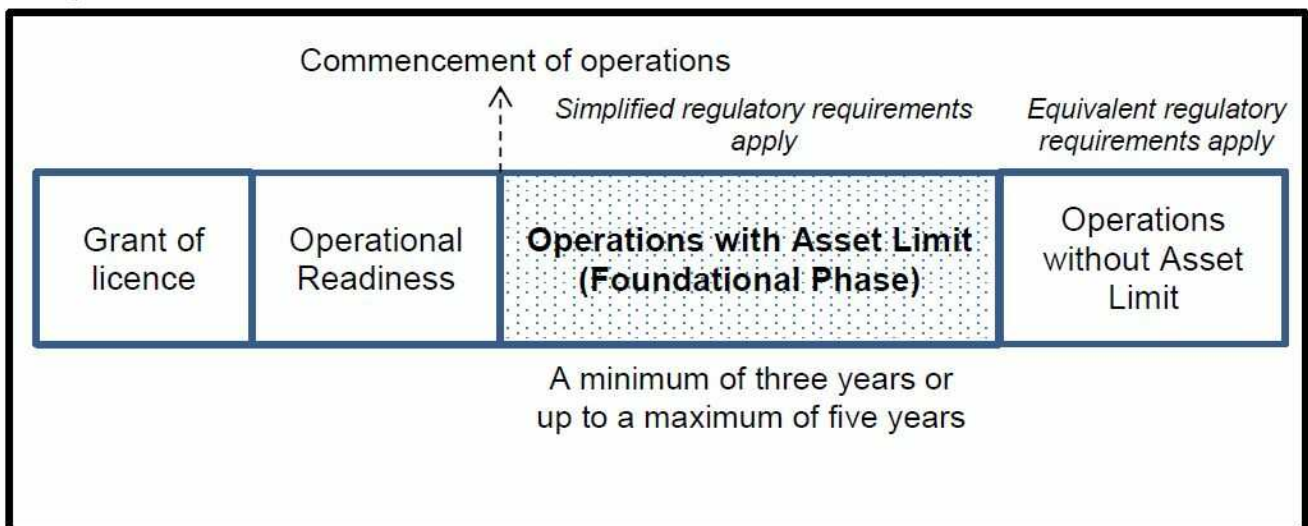
26. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) paras 7.2 and 7.3
27. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 1.6
28. Bank Negara Malaysia, *Application Procedures for New Licences under Financial Services Act 2013 and Islamic Financial Services Act 2013: Exposure Draft* (BNM/RH/PD 030-4, 27 December 2019) para 1.3 and 1.4
29. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 7.2



What happens at the end of the foundational phase?

1. A licensed digital bank may after three (3) years from the commencement of its operations, submit to the Bank for the foundational phase to end and for the business limitation to be uplifted.
2. The Bank will assess whether the licensed digital bank has:-
 - a. complied with all applicable laws and regulatory requirements;
 - b. **achieved a minimum amount of capital funds of RM300 million;** and
 - c. shown satisfactory progress in achieving the committed value propositions as described in its business plan.
3. If all of the above is achieved by the end of the fifth year from the commencement of their operation, the business limitation shall no longer be applicable.
4. Failing to fulfil any of the requirements by the end of the fifth year from the commencement of their operation, the licensed digital bank may be subject to an enforcement action, including a direction to implement its exit plan or revocation of license.
5. The licensed digital bank is expected to continue serving the underserved or unserved segments as part of its business operations, even after the end of the foundational phase.

Diagram 1: Timeline



Source: Bank Negara Malaysia



31

How do I facilitate the business of paying or collecting cheques?

1. Appoint another licensed bank or licensed Islamic bank that is an e-SPICK member to manage the physical collection of cheques.
2. Use technology to minimise the physical collection of cheques, subject to adequate safeguards.

Will I need to set up a registered office in Malaysia³²

Yes. This is to ensure that its sole registered office allows the Bank to communicate with the licensed digital bank during the supervisory process.

32

Are physical access points allowed?

The licensed digital bank will not be allowed to establish physical branches but may participate in the Shared ATM Network and any other cash-out services offered by PayNet. Financial services through agents are permitted, subject to the Bank's approval.

31. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 16.1

32. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 17.1-17.4



Key Comments on Bank Negara's e-KYC Exposure Drafts



*Er Chiang Kai,
CTO of V-KEY*

The Exposure Draft needs to consider security requirements for mobile apps

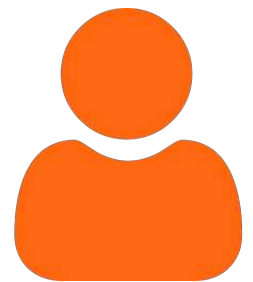
As mobile apps will serve as the main touch points for users of digital banks, there should be requirements on the security of such apps, with built-in tamper protections as well as multi-factor authentication.

A licensed digital bank should have clearly-defined social obligations to protect the consumer

A licensed digital bank should protect customers against social engineering attacks (e.g., phishing), through technology and education. As far as possible, a licensed digital bank should also minimise the use of special end-user device features so that the use of the digital bank app can be ubiquitous.

What is the manpower requirement like for digital banks?

Prospective applicants are required to indicate the talent requirement (as per the business plan) over the five-year period and how the required numbers and skills will be met in areas related to technology and risk management, and where applicable, requisite Shariah expertise. Would there be a requirement to hire local talents and is there a percentage to be fulfilled by digital banks? Would this also apply to local shareholdings and/or directors?



Industrial Expert



Considerations for the Future





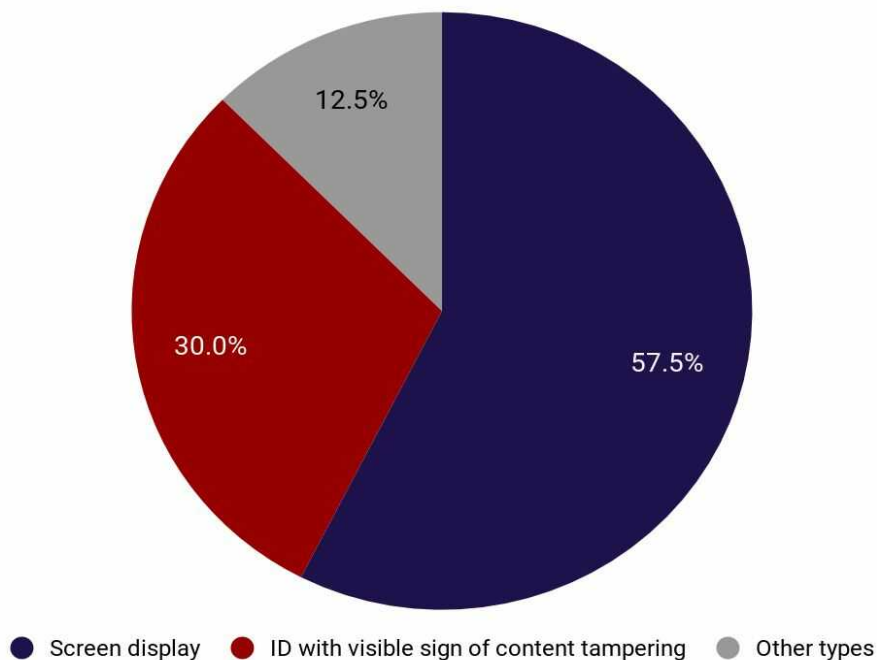
Do we have enough data to support the implementation of e-KYC and Digital Banks?

New technologies such as e-KYC solutions and digital banks require data sources that are able to verify customer information. Although the National Identity Card (MyKad) is one of the main sources for reliable data, its **reliability cannot be guaranteed in the online sphere**. Unlike **conventional ID verification** where the card is **physically processed by a machine or human**, **digital processing relies heavily on the customer's input** (e.g. clarity of photo, and positioning) and technologies implemented (e.g. OCR systems, camera lenses, and software systems).

Statistics on Malaysia's e-KYC implementation for mobile network operators³³

After 2 years of e-KYC implementation for mobile network operators in Malaysia, Innov8tif has observed that non-compliant MyKad document images constitute 1.72% of 100,000 audited cases.

- i. **Screen-display** (ID presented from screen) tops the chart at 57.5%;
- ii. Followed by **ID with visible sign of content tampering** at 30%; and
- iii. **Other types** of uncompiled MyKad images identified were photocopy document, color-printed copy, incomplete image, blurred image, partially-damaged document and hidden ID photo.



Source: Innov8tif

33. Information is provided exclusively by Innov8tif. You may learn more about them at <https://innov8tif.com/>



Cost Savings in Indonesia

In Indonesia, having third-party verification providers who have access to a national digital identity system allowed compliance costs to be reduced by 70-80%.

Source: Securemetric

In other countries like the Netherlands (DigiD) and Singapore (SingPass), a national digital identity system exists where customers are able to transact digitally with the government and private sector in a convenient and secure manner. If Malaysia were to implement digital banks, the marriage of both a front-end plug (e-KYC) and backend database storage (national digital identity system) is necessary.³⁴

This begs the question ...



Frederic Ho,
VP of Jumio,
APAC Region

Should we wait for a national digital identity system before we consider implementing e-KYC and digital banks?

Having it first is ideal but there are other countries who have implemented them without having a fully-fledged (e.g. fingerprint database) national digital identity system. In Australia, the government relies on their Document Verification Service (Australian Post's digital iD) to compare a customer's identifying information with a government record instead of biometrics. We should leverage on what we have and launch or this will be a honeypot of centralised national personal data for data breaches and cybersecurity attacks if we are not ready with the necessary robust talents and platform.

34. Frederic Ho, VP of Jumio, APAC Region



How should we store and process the data required for the implementation of e-KYC and Digital Banks

Cumulations of vast volume of data are both necessary and a natural byproduct of a digital economy. **Traditionally, businesses have to buy their own hardware and software to manage their own data centers** (e.g. in-house servers and private networks). But as technology advances, new services such as cloud technology are fast becoming the prevailing form of computing services.



What is cloud technology?

In simple terms, cloud computing is the **on-demand delivery of IT resources over the Internet with pay-as-you-go pricing**.³⁵ Instead of building their own system, businesses subscribe to a cloud provider and pay for their services whereby the cloud provider will be responsible for managing the servers, storage, databases, networking, software, analytics, and intelligence - the subscriber will typically pay only for what they need without bearing the costs of capital investment and the associated fixed costs (e.g. electricity and IT experts).³⁶

Businesses are eyeing cloud because of its potential to scale, improve performance, improve reliability, and its cost-saving implications. Digital banks, in particular, will benefit from the use of cloud services because of their newness to the market (minimising capital risks). However, there are also **concerns about cloud technology and its security risks**. Both businesses and regulators have to work together and decide which form of data management is the most practicable, cost-effective, and secure solution.

Key issues for consideration:

1. What kind of data management solutions that smaller companies (e.g. FinTech startups) leverage on to upscale themselves and compete with bigger institutions (e.g. established banks)?
2. Are residential data centers more secure than cloud services?
3. What are the key differences in terms of risks, implementation and cost-benefit analysis when it comes to public, hybrid and private cloud services?
4. Is there any difference (jurisdictionally) where data is processed/stored? If there is a difference, how should the data be segregated?
5. If there are leakages/data breaches, who would be liable? Would liabilities be affected or separated if different parties are processing and storing the data?
6. Should there be more specific or detailed guidelines on cloud apart from the one highlighted in Policy Document on Risk Management in Technology (RMiT) (issued on 18 July 2019) (and Policy Document on Outsourcing (issued on 23 October 2019)?

35. Amazon Web Services, 'What is cloud computing?' (AWS) <<https://aws.amazon.com/what-is-cloud-computing/>> accessed 8 February 2020

36. Microsoft Azure, 'What is cloud computing?' (Microsoft) <<https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/>> accessed 8 February 2020



What is the right balance between automation and human intervention?

Whether it is through AI or predictive algorithms, **both e-KYC solutions and digital banks will almost definitely rely on some form of automation.** The question then becomes, how can we best maximise automation whilst minimising manual intervention and fraud?

Maintaining the balance: A Malaysian Perspective ³⁷

Consumers will not be eligible for straight-through or system-automated onboarding. Consistently among multiple implementations, Innov8tif observed that:



“Good”
Cases

About half (between 50-60%) of the users were eligible to satisfy all required thresholds set in system-automated ID verification, and thus could be onboarded without human intervention.



“Require
Further
Review”
Cases

Approximately 30-35% of the users fell under the “neither too good nor too bad” category. Facial biometrics verification were satisfied, and there was no visible sign of content tampering on identity document. However, the quality of identity document was poor and did not satisfy minimum scorecard threshold configured for document authentication. This category can be further reviewed through the funnel by (1) requesting for the 2nd officially valid document (OVD) such as driver’s license and passport, (2) going through review and decision making process by compliance team or authorised examiner (i.e. eye-balling), or (3) verifying a person’s identity through 3rd party data source or knowledge base.



“Bad”
Cases

The remaining 10-15% users were outright declined, due to failure in satisfying liveness detection, 1-to-1 face comparison against ID photo, or non-compliant identity document images. The size of this category was primarily driven by the incentives to attempt fraudulent ID, such as new-user promotions or user referral campaigns.

Source: Innov8tif

It is difficult to say where the threshold should be - it ultimately **boils down to the availability of data and the types of technologies utilised.** Regardless, a wider perspective from what is practicable for a business needs to be taken into account. ³⁸

37. Information is provided exclusively by Innov8tif. You may learn more about them at <https://innov8tif.com/>
38. Frederic Ho, VP of Jumio, APAC Region



Do we have sufficient talent and knowledge to meet the long-term demands of the FinTech industry?

During the private roundtable discussion on 6 Feb 2020, there was **broad consensus from industry experts** on the **lack of talents** that would be sufficient to sustain the FinTech market in Malaysia; **the rapid pace at which technology develops is outpacing the labour market**. As such, this could **potentially lead to increased competition over a limited talentpool**.

A global war for talent ...

There is a growing demand for new and emergent skills which the labour market cannot meet. In a survey conducted by PwC, **eight out of 10 global CEOs have voiced out their concern for the lack of people with the right skills**.³⁹ Such fears cultivate short-term strategies where many **employers are willing to spend exorbitant amount of money on recruiting (or poaching)**, while **reluctant to invest in training their existing workers or unskilled ones**. Spending per employee (estimated at \$1,000 per annum) is significantly less than cost-to-hire (estimated at \$4,000 per annum) - this is likely fuelled by the fear of being victimised through poaching from other companies.⁴⁰

... can already be seen in Malaysia's financial industry

41

In 2018, the Bank warned **financial institutions not to "wholesale pinch" staff from each other**. Despite the warning, the **practice is still pervasive throughout the industry**, where pinching efforts have become more common in higher-demand areas like risk management and compliance. **Banks are left with no choice but to pinch** because they **do not have the time to train a person to meet the necessary level of expertise**. Moreover, there is a ripple effect where key employees who leave are likely to be followed by those that worked with them.

So what is the game plan for Malaysia's FinTech talents?

Planning for human capital is vital in the FinTech industry and would require **strong support from both the regulators and the private sector**. This needs to be **addressed quickly** as the **market size for FinTech is growing at an unprecedented rate**.

39. PwC, 'Talent trends 2019: Upskilling for a digital world' (PwC's 22nd Annual Global CEO Survey trends series, January 2019) <<https://www.pwc.com/gx/en/ceo-survey/2019/Theme-assets/reports/talent-trends-report.pdf>> accessed 8 February 2020

40. Seth Haris and Jake Schwartz, 'Why Competing for new Talent is a Mistake' (Harvard Business Review, 5 February 2020) <https://hbr.org/2020/02/why-competing-for-new-talent-is-a-mistake?utm_source=linkedin&utm_campaign=hbr&utm_medium=social> accessed 8 February 2020

41. Adeline Paul Raj, 'Newsbreak: Banks told not to pinch staff wholesale' (the Edge, 30 April 2018) <<https://www.theedgemarkets.com/article/newsbreak-banks-told-not-pinch-staff-wholesale>> accessed 9 February 2020



Market size for digital transactions



The market's largest segment is **Digital Payments** with a total transaction value of **US\$12,406m in 2020** and is expected to show an annual growth rate (CAGR 2020-2023) of 10.8% resulting in the total amount of US\$16,860m by 2023



Total transaction value in the **Personal Finance** segment amounts to **US\$599m in 2020** and is expected to show an annual growth rate (CAGR 2020-2023) of 23.8% resulting in the total amount of US\$1,135m by 2023.



Transaction value in the **Digital Remittances** segment amounts to **US\$492m in 2020** and is expected to show an annual growth rate (CAGR 2020-2023) of 19.6% resulting in the total amount of US\$841m by 2023.



Assets under management in the **Robo-Advisors** segment amounts to **US\$107m in 2020** and is expected to show an annual growth rate (CAGR 2020-2023) of 40.2% resulting in the total amount of US\$294m by 2023.

Source: Statista⁴²

A Securities Commission Approach ...

One notable practice from the Securities Commission is that they **require recognised market operators** (RMO) who operate in Recognised Markets (equity crowdfunding, peer-to-peer financing, digital asset exchange, and property crowdfunding) **to carry out continuous awareness and education programmes**.⁴³ Perhaps similar obligations could be imposed for e-KYC solutions and digital banks?

42. Statista, 'FinTech - Malaysia' <<https://www.statista.com/outlook/295/122/fintech/malaysia>> accessed 9 February 2020

43. Securities Commission Malaysia, *Guidelines on Recognised Markets* (SC-GL/6-2015(R3-2019), revised 17 May 2019) section 6.01(h)



Featured Companies





REFINITIVTM



Website: <https://www.refinitiv.com/>

Refinitiv is one of the world's largest providers of financial markets data and infrastructure, serving over 40,000 institutions in approximately 190 countries. We provide leading data and insights, trading platforms, and open data and technology platforms that connect a thriving global financial markets community - driving performance in trading, investment, wealth management, regulatory compliance, market data management, enterprise risk and fighting financial crime.

Refinitiv's World-Check is a highly structured database of intelligence on heightened risk individuals and organizations. Widely adopted by financial services companies, it supports the KYC and Third-Party Risk due diligence process and helps uncover risks associated with sanctions, organized crime, fraud, money laundering, bribery and corruption, as well as modern day slavery and country risk.

According to Refinitiv's annual financial crime report 2019, three-quarters of Asia Pacific organizations have been affected by financial crime over the past 12 months, leading to 60% of these businesses adopting new technologies to combat the issue.

OVO, Indonesia's leading digital payments platform, has selected Refinitiv's World-Check to support its Know-Your-Customer (KYC) and Anti-Money Laundering (AML) procedures to minimize its exposure to financial crime risks. This partnership comes at a time when OVO looks to continue the expansion of its business and to drive financial inclusion across the country.



JUMIO[®]

Website: <https://www.jumio.com/>

Jumio is the global leader in the identity verification space. Jumio's online ID and Identity Verification solutions allows businesses to establish the genuine identity of their users by verifying the authenticity of the government-issued IDs in real time and matching the selfie photo with the ID photo to ensure that the person holding the ID is the same person. This combination, coupled with certified liveness detection and advanced anti-spoofing technology, provides strong defence against identity fraud and deepfakes.

Jumio supports more than 3,500 ID types across 200 countries and territories and delivers the highest accuracy rates in the industry, which translates to lower operating costs and manual reviews. We process close to 300,000 verifications every day and have built a massive database of attempted fraud over time. Coupling with AI and machine learning, we're training our ML algorithms to more accurately identify fraud and detect fraud patterns.



V-KEY

STRONGER WITH V-OS

Website: <https://www.v-key.com/>

V-Key is an internationally-acclaimed software-based digital security company, headquartered in Singapore. V-Key's pioneering technology powers ultra-high-security solutions for digital identity management, user authentication and authorization, as well as electronic payments for major banks, payment gateways, and government agencies.

V-Key is the inventor of V-OS, the world's first Virtual Secure Element. Internationally patented, V-OS uses advanced cryptographic and cybersecurity protections to comply with standards previously reserved only for expensive hardware solutions. Today, V-OS secures millions of users around the world.

V-OS enables digital leaders to create powerful customer experiences that combine high security and delightful convenience. V-OS integrates seamlessly with biometrics, PKI-based technology, out-of-band authentication, making delightful user experiences possible while being uncompromisingly secure.

V-OS is FIPS 140-2 Validated (US NIST) and accredited by the Infocomm Media Development Authority of Singapore (IMDA). V-OS has been the subject of multiple rigorous penetration tests and has been stress-tested by e-commerce players, government agencies, regulatory bodies and financial services companies.



**SECURE
METRIC**
TECHNOLOGY

Website: <https://www.securemetric.com/>

Securemetric Berhad is a digital security company founded in **Malaysia** with a mission in "Securing World Digital Economy Transformation for today and tomorrow". We build solutions in Securing Digital Identity, Securing Payment Transaction and Securing Application Solution. Securemetric has regional office in Philippines, Vietnam, Indonesia and Singapore.

Securemetric specializes in building **Enterprise Certificate Authority (CA)** and **National Public Key Infrastructure (PKI)** for large corporate and government agencies. PKI is the fundamental infrastructure in all facets of digitization ecosystem that requires Authentication, Encryption and Non-Repudiation Policy in Digital Signature's compliances.

In Authentication business, Securemetric research and develop CENTAGATE® Centralized Authentication Gateway to secure and enable Identity Management. It is featured with Multi-Factor Authentication (MFA), Single Sign On (SSO), and Transaction Signing. This MFA solution is further enhanced with Adaptive Intelligence capabilities and Risk Scoring Engine to proactive and self-defending Identity security. CENTAGATE is the first in South East Asia with FIDO2 certification, and is being used by top-tier banks in the Philippines, Indonesia and Vietnam.

In Digital Signature landscape, Securemetric launched its first Cloud-base digital signature platform called **SigningCloud**. This is an Electronic Document Management Platform that provides PKI digital signature capabilities with trusted third-party digital certificate, thus it is in compliance to eIDAS Regulation and Digital Signature Act 1997. SigningCloud is integrated with Digital Customer Onboarding (eKYC) by Innov8tif and API integration with Joget Workflow. With this integration, SigningCloud provides a seamless user experience for business users to authenticate identity, working on documents work-flow, and managing digital signature request and approval process..



innov8tif

Website: <https://innov8tif.com/>

Innov8tif (pronounced “innovative”) is a software technology company set with a common goal of helping businesses to realise digitalisation roadmap - both in customer onboarding experience and operational efficiency. Innov8tif’s EMAS eKYC product provides digital ID verification to support online customer onboarding process and identity fraud management. EMAS eKYC was accorded Merit for B2B Fintech category at the 19th Asia Pacific ICT Alliance Awards (APICTA Awards).

Headquartered in Malaysia since 2011, Innov8tif has expanded its market presence in the South East Asia region. Built on years of trusted relationship, Innov8tif’s clientele comprises the telecommunication companies, BFSI (banking, financial services & insurance) industries, multinational manufacturing companies and government agencies. Amongst, many are public listed corporates.



GHL the ASEAN payment people

Website: <https://www.ghl.com/>

At the forefront of ASEAN cutting edge Fintech, GHL empowers the payment revolution that is shaping our spending habits today. From new generation cashless to personalized-value added solutions, we offer extensive payment options, both offline and online to fulfil your customers' needs. GHL aspires to uplift businesses byway of upgrading their transactional operations, while delivering convenience to consumers to enhance their shopping experience. With over 25 years' worth of expertise to enrich our portfolio we are now in presence across 7 countries; Malaysia, Thailand, Philippines, Indonesia, Cambodia, Singapore, and Australia.

1. Transaction Payment Acquisition

a. Card Payment

Dubbed as ASEAN's principal Third Party Acquirer in ASEAN, we represent major financial institutions and locally as well as globally reputed payment schemes.

b. Payment Collection

We are Malaysia's largest reload and bill collection network under the emblem of well-recognized purple logo, e-pay processes a total of over 30 million transactions, amounting up to RM350 million in value, nationwide per month.

c. Next Generation Payment

Riding the Asian cashless tide, alongside with significant Asian mobile/digital payment players, we include major local and cross border e-wallets' acceptance across our footprint.

d. Internet Payment Solution

Our online payment arm - eGHL offers secure internet payment gateway covering both card and non-card payment channels, and online businesses throughout the ASEAN region.

2. Shared Services:

GHL provides Android All-in-One Point of Sales (POS) terminals and other payment acceptance devices that can perform numerous electronic payments for credit cards, debit cards, e-wallets, loyalty points' capture, redemption transactions, loan repayments, and other bank/merchant specific requirements. These devices offered are either on a sale, lease, rental, and/or maintenance basis.

3. Solution Services:

GHL offers extensive loyalty and prepaid e-wallet solution that supports the collection and redemption of loyalty points, prepaid e-wallet, and gift card payments. GHL also offers a secure 'PCI-DSS-compliant' payment network that supplies both software and hardware solutions, on top of customised internet payment solution.



LAWTECH
MALAYSIA

3
2

Moving Forward





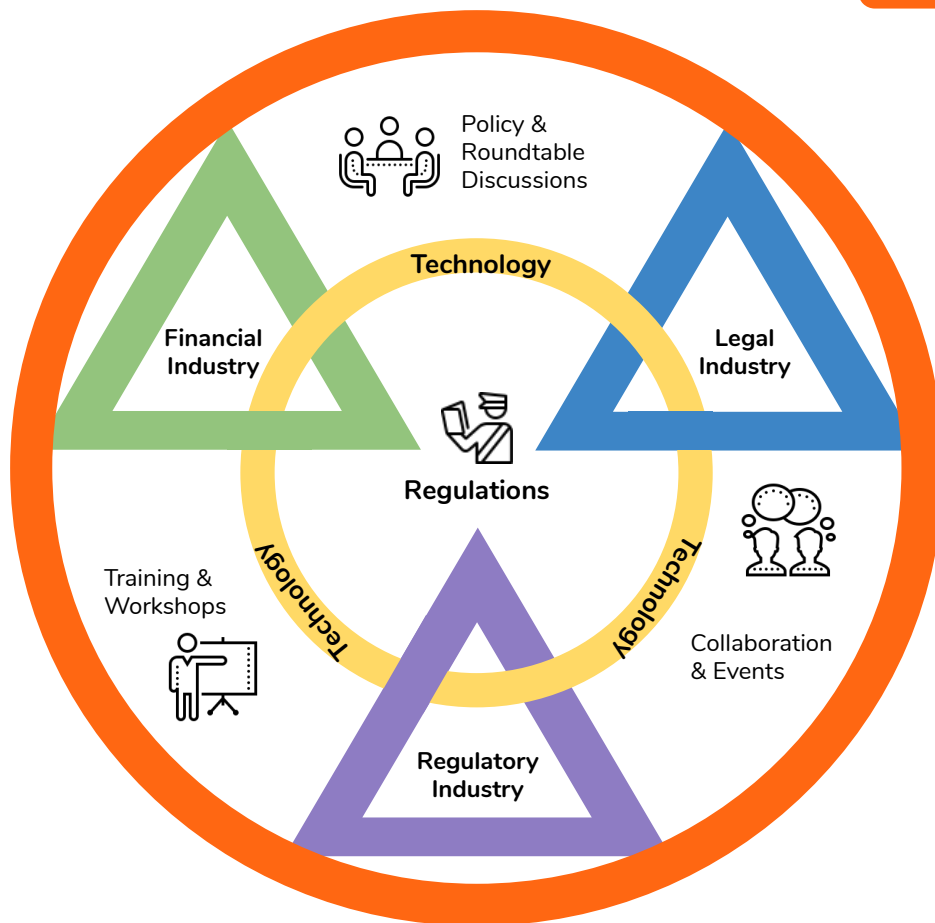
We must take more action to get ready for digital transformation and create a sustainable robust FinTech ecosystem. Convergence between the financial, legal, and regulatory industries that is...

... supported by the community

...underpinned by technology

...and centered around robust regulations

...is crucial



Source: LTM (LawTech Malaysia)

We look forward to ...

- more industry talks that covers specialised fields within the FinTech industry
- more creative efforts nationwide that tackles the talent issue
- more insights, research and content-sharing that addresses different issues and democratises FinTech knowledge for both technical and non-technical audiences



References





1. Bank Negara Malaysia, Financial Technology Regulatory Sandbox Framework (BBNM/RH/PD 030-1, 18 October 2016)
2. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019)
3. Bank Negara Malaysia, Licensing Framework for Digital Banks: Exposure Draft (BNM/RH/ED 030-3, 27 December 2019)
4. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 5.2
5. Frederic Ho, VP of Jumio, APAC Region
6. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 5.2
7. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 5.2
8. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 10.1
9. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.1
10. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.2
11. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.3
12. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.6
13. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.10
14. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.11
15. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.8
16. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) Appendix 1, para 3
17. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.13
18. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) para 7.3 (ibid 11)
19. Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) Exposure Draft (BNM/RH/ED 030-2, 16 December 2019) Appendix 2, para 1
20. Anatoly V Zhuplev, Disruptive Technologies for Business Development and Strategic Advantage (IGI Global, 22 June 2018)



21. Antony Jenkins, 'The demise of the traditional banking model is actually good news for all of us' (Quartz, 27 November 2019)
<<https://qz.com/1755889/the-democratic-benefits-of-digital-banking/>> accessed 8 February 2019
22. Bank Negara Malaysia, 'Exposure Draft on Licensing Framework for Digital Banks: Press Release' (27 December 2019)
<https://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4970> accessed 9 February 2020
23. Do take note that there are other policy documents that have been issued by the Bank to supplement this exposure draft which are Bank Negara Malaysia, *Application Procedures for Acquisition of Interest in Shares and to be a Financial Holding Company* (BNM/RH/PD 030-5, 27 December 2019) and Bank Negara Malaysia, *Application Procedures for New Licences under Financial Services Act 2013 and Islamic Financial Services Act 2013* (BNM/RH/PD 030-4, 27 December 2019)
24. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 2.1.
25. Objectives were derived from the overarching principles contained in both the Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) and Bank Negara Malaysia, 'Exposure Draft on Licensing Framework for Digital Banks: Press Release' (27 December 2019)
<https://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4970> accessed 9 February 2020
26. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) paras 7.2 and 7.3
27. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 1.6
28. Bank Negara Malaysia, *Application Procedures for New Licences under Financial Services Act 2013 and Islamic Financial Services Act 2013: Exposure Draft* (BNM/RH/PD 030-4, 27 December 2019) paras 1.3 and 1.4
29. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 7.2
30. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) paras 15.1-15.5
31. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 16.1
32. Bank Negara Malaysia, *Licensing Framework for Digital Banks: Exposure Draft* (BNM/RH/ED 030-3, 27 December 2019) para 17.1-17.4
33. Information is provided exclusively by Innov8tif. You may learn more about them at <https://innov8tif.com/>
34. Frederic Ho, VP of Jumio, APAC Region (ibid 5)
35. Amazon Web Services, 'What is cloud computing?' (AWS)
<<https://aws.amazon.com/what-is-cloud-computing/>> accessed 8 February 2020
36. Microsoft Azure, 'What is cloud computing?' (Microsoft)
<<https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/>> accessed 8 February 2020
37. Information is provided exclusively by Innov8tif. You may learn more about them at <https://innov8tif.com/> (ibid 33)



38. Frederic Ho, VP of Jumio, APAC Region (ibid 33)
39. PwC, 'Talent trends 2019: Upskilling for a digital world' (PwC's 22nd Annual Global CEO Survey trends series, January 2019)
<<https://www.pwc.com/gx/en/ceo-survey/2019/Theme-assets/reports/talent-trends-report.pdf>>
> accessed 8 February 2020
40. Seth Haris and Jake Schwartz, 'Why Competing for new Talent is a Mistake' (Harvard Business Review, 5 February 2020)
<https://hbr.org/2020/02/why-competing-for-new-talent-is-a-mistake?utm_source=linkedin&utm_campaign=hbr&utm_medium=social> accessed 8 February 2020
41. Adeline Paul Raj, 'Newsbreak: Banks told not to pinch staff wholesale' (the Edge, 30 April 2018)
<<https://www.theedgemarkets.com/article/newsbreak-banks-told-not-pinch-staff-wholesale>>
accessed 9 February 2020
42. Statista, 'FinTech - Malaysia' <<https://www.statista.com/outlook/295/122/fintech/malaysia>>
accessed 9 February 2020
43. Securities Commission Malaysia, Guidelines on Recognised Markets (SC-GL/6-2015(R3-2019), revised 17 May 2019) section 6.01(h)



LAWTECH
MALAYSIA

3
8

Contact Us



Details

Email : info@lawtech.my
Website : www.lawtechmalaysia.com
Event website : www.supernovasummit.com