BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Electronic Know-Your-Customer (e-KYC)

Exposure Draft

Applicable to:

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
9. Approved non-bank issuers of designated payment instruments and designated Islamic payment instruments

Draft issued on: 23 February 2023

This exposure draft sets out the proposed enhanced requirements and guidance in implementing electronic Know-Your-Customer (e-KYC) solutions for the on-boarding of individuals and legal persons to the financial sector.

The proposals in this exposure draft seek to accommodate advancements in technology to facilitate secure and safe adoption of e-KYC solutions for both individuals and legal persons, while preserving the integrity of the financial system.

Bank Negara Malaysia invites written feedback on the proposals in this exposure draft, including suggestions on areas to be clarified and alternative proposals that the Bank should consider. The written feedback should be supported with clear rationale, accompanying evidence or appropriate illustrations to facilitate an effective review of this exposure draft.

Feedback must be submitted by **2 May 2023** to:

Pengarah,
Jabatan Pembangunan dan Inovasi Kewangan
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: e-kycpolicy@bnm.gov.my

Electronic submission is encouraged. Submissions received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

In the course of preparing your feedback, you may direct any queries to e-kycpolicy@bnm.gov.my

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 Supported by further technological advancements and introduction of electronic Know-Your-Customer (e-KYC) solutions for the financial sector, digitalisation of the customer identification and verification processes has become an increasingly prominent enabler in the onboarding process of financial services.

1.2 Growing adoption and understanding of e-KYC solutions in the financial sector call for enhancements to existing requirements to ensure e-KYC solutions continue to remain relevant, robust and reliable. This includes expanding the scope of e-KYC applications to cover both individuals and legal person, providing guidance on e-KYC solutions that can cater to the unbanked, while ensuring uncompromised accuracy in customer identification and verification.

1.3 This document sets out the minimum requirements and standards that a financial institution, as defined in paragraph 5.2, must observe in implementing e-KYC for the on-boarding of individuals and legal persons. The requirements outlined in this policy document are aimed at-

(i) Enabling safe and secure application of e-KYC technology in the financial sector;
(ii) Facilitating the Bank's continued ability to carry out effective supervisory oversight over financial institutions; and
(iii) Ensuring effective anti-money laundering and countering financing of terrorism (AML/CFT) control measures.

2 Applicability

2.1 This document is applicable to all financial institutions as defined in paragraph 5.2 and any other institution that may be specified by the Bank.

2.2 This policy document shall not apply to agent banking channels governed under the Agent Banking policy document dated 30 April 2015.

3 Legal provisions

3.1 This policy document is issued pursuant to-

(i) sections 47(1) and 261(1) of the Financial Services Act 2013 (FSA);
(ii) sections 57(1) and 272 of the Islamic Financial Services Act 2013 (IFSA);
(iii) sections 41(1),126 and 123A of the Development Financial Institutions Act 2002 (DFIA);
(iv) sections 74 of the Money Services Business Act 2011 (MSBA); and
(v) sections 16 and 83 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA).

4 Effective date

4.1 This policy document comes into effect on [*a date to be specified in the final policy document*]

5 Interpretation

5.1 The terms and expressions in this policy document shall have the same meaning assigned to them in the FSA, IFSA, DFIA, AMLA and MSBA unless otherwise stated.

5.2 For the purposes of this policy document-

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action.

"**G"** denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted.

"the Bank" means Bank Negara Malaysia.

"financial institution" refers to-
(i) a licensed bank, investment bank and life insurer under the FSA;
(ii) a licensed Islamic bank and licensed family takaful operator under the IFSA;
(iii) a prescribed development financial institution under the DFIA;
(iv) an approved non-bank issuer of designated payment instruments under the FSA;
(v) an approved non-bank issuer of designated Islamic payment instruments under the IFSA; and
(vi) a licensed money-changing operator and/or a licensed remittance service provider under the MSBA.

"authorised person" refers to a natural person appointed in writing[1] by a legal person to operate and maintain an account with a financial institution including to open, close and give any instruction for the conduct of financial transactions in the account on behalf of the legal person.

"biometric" refers to a unique physical feature of a person based on a certain aspect of the person's biology. These include facial features, fingerprints or retinal patterns.

"Board" in relation to a company, refers to-

[1] By means of a letter of authority or directors' resolution or by electronic means, as permitted under the legal person's constitution. For avoidance of doubt, requirements relating to such electronic means can be referred in paragraph 8.11 of this policy document.

(i) directors of the company who number not less than the required quorum acting as a board of directors; or
(ii) if the company has only one director, that director.

"legal person" means a legal person as specified under paragraph 6.2 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs) policy document. It refers to any entity other than a natural person that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, government-linked companies (GLC), foundations, partnerships, or associations and other similar entities.

GLC refers to an entity where the government is the majority shareholder or single largest shareholder and has the ability to exercise and/or influence major decisions such as appointment of board members and senior management.

"customer" refers to both account holder and non-account holder. The term also refers to a client.

For the life insurance and family takaful sector, "customer" refers to parties related to an insurance/takaful contract including potential parties such as proposer/policyholder/policy owner, payor, assignee and company representative, but does not include insurance agent.

In the case of group policies, "customer" refers to the master policy holder, that is, the owner of the master policy issued or intended to be issued.

In addition, for money service business and non-bank issuers of designated payment instruments, "customer" refers to a person for whom the licensee or approved persons undertakes or intends to undertake business transactions.

Where the term "customer" is broadly used in this policy document, requirements shall apply to both individual and legal person.

"**beneficial owner"** refers to any natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person or arrangement.

Reference to "ultimately owns or control" or "ultimate effective control" refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.

In insurance and takaful sectors, this also refers to any natural person(s) who ultimately owns or controls a beneficiary, as specified in the AML/CFT and TFS for FIs policy document.

"electronic Know-Your-Customer (e-KYC)" means establishing business relationships and conducting customer due diligence (CDD)[2] by way of electronic means, including online channel and mobile channel.

"False Positive" refers to identification and verification cases processed under e-KYC solutions in which the solution accepted and verified an identity when said identity should have been rejected. These include cases of false or unclear identities, forged or tampered documents and unclear images that were wrongly accepted.

"False Negative" refers to identification and verification cases processed under e-KYC solutions in which the solution wrongly rejected and did not verify an identity when it should have been accepted. These include cases of genuine identities or documents that were wrongly rejected.

"True Positive" refers to identification and verification cases processed under e-KYC solutions in which the solution rightly accepted and verified an identity. These include cases of genuine identities or documents that were rightly accepted.

"True Negative" refers to identification and verification cases processed under e-KYC solutions in which the solution rightly rejected and did not verify an identity. These include cases of false or unclear identities, forged or tampered documents and unclear images that were rightly rejected:

"individual" refers to a natural person.

Question 1:
Does the definition of "legal person" and "authorised person" in this Policy Document sufficiently capture the intended target market(s) for businesses to be on-boarded through e-KYC?

6 Related legal instruments and policy documents

6.1 Where applicable, this policy document must be read together with any relevant legal instruments, policy documents, guidelines, circulars, and supplementary documents issued by the Bank, in particular-

(i) AML/CFT and TFS for FIs policy document issued on 31 December 2019;
(ii) AML/CFT and TFS for FIs (Supplementary Document No. 1) – Money Services Business Sector issued on 30 June 2021
(iii) Risk Management in Technology (RMiT) dated 19 June 2020;
(iv) Outsourcing dated 23 October 2019;
(v) Management of Customer Information and Permitted Disclosures dated

[2] This includes cases of standard and simplified CDD on individuals, legal persons and beneficiaries as specified under the AML/CFT and TFS for FIs policy document.

12 October 2021;
(vi) Introduction of New Products dated 7 March 2014; and
(vii) Introduction of New Products by Insurers and Takaful Operators dated 15 May 2015.

7 Policy documents superseded

7.1 This policy document supersedes the Electronic Know-Your-Customer (e-KYC) policy document issued on 30 June 2020.

PART B POLICY REQUIREMENTS

8 e-KYC implementation

Role and responsibility of the Board

S 8.1 A financial institution shall obtain Board approval on the overall risk appetite and internal framework governing the implementation of e-KYC for both individuals and legal persons. The framework shall address-

i. high risk or material risk scenarios that require subsequent Board approval;
ii. variations or exceptions to existing e-KYC related products or methods that require subsequent Board approval; and
iii. other instances that require Board approval.

S 8.2 The Board of a financial institution shall set and 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/TF) risks.

Identification and verification (IDV) of customers through e-KYC

A. General requirements

S 8.3 A financial institution shall ensure and be able to demonstrate on a continuing basis that appropriate measures for the identification and verification of a customer's identity through e-KYC are secure and effective[3].

S 8.4 A financial institution shall adopt an appropriate combination of authentication factors when establishing measures to verify the identity of a customer being on-boarded through e-KYC. The strength and combination of the authentication factors shall be commensurate to the risks associated with inaccurate identification for a particular product or service.

G 8.5 In respect of paragraph 8.4, a financial institution may give regard to the key basic authentication factors, namely and amongst others, something the customer possesses (e.g. identity card, registered mobile number, company's certificate of incorporation) and something the customer knows (e.g. PIN, personal information, credit history). In the case of individuals, this should include something the customer is (e.g. biometric characteristics). An e-KYC solution that depends on more than one factor is typically more difficult to compromise than a single factor system.

[3] Measures for identification and verification should be proportionate to the risk dimensions of e-KYC. Where reference is made to face-to-face processes, this should mainly serve as a guide on the minimum expected baseline.

B. IDV through e-KYC for individuals

G 8.6 In identifying and verifying an individual's identity through e-KYC as required by the AML/CFT and TFS for FIs policy document, a financial institution may undertake measures including but are not limited to the following-

(i) verifying the customer against a government issued ID by utilising biometric technology;

(ii) ensuring that the government issued ID to support e-KYC customer verification is authentic by utilising appropriate fraud detection mechanisms; and/or

(iii) ensuring the customer is a live subject and not an impersonator (e.g. through use of photos, videos, synthetic human face masks[4]) by utilising liveness detection.

Question 2:
Are there any other relevant key considerations in identifying and verifying an individual customer's identity through e-KYC that should be included in this policy document, including those based on newer technology or practices? If yes, please indicate and elaborate how these considerations may contribute towards secure identification and verification.

C. IDV through e-KYC for legal person[5]

G 8.7 A financial institution may implement e-KYC to identify and verify legal persons, subject to meeting the requirements in this policy document and the requirements for legal persons specified under the AML/CFT and TFS for FIs policy document[6] on CDD for legal persons.

S 8.8 When implementing e-KYC for legal persons, a financial institution shall have due regard to the areas listed as CDD requirements for legal persons in the AML/CFT and TFS for FIs Policy Document. This includes but are not limited to-

(i) identification and verification of a legal person as an entity to establish the existence of a legitimate business[7].

(ii) identification and verification of the authorised person appointed by the legal person to establish business relations and conduct transactions on

[4] Synthetic human face masks are designed to impersonate real human faces and made from materials such as silicone or otherwise. For purposes of e-KYC, such masks may be used to defraud facial recognition software.

[5] For avoidance of doubt, a sole proprietor is not deemed as legal person under this policy document. Accordingly, the on-boarding of sole proprietors through e-KYC is subject to e-KYC process for individual as specified under para 8.6.

[6] In particular, requirements relating to legal persons as well as clubs, societies and charities contained within paragraphs 14A.9, 14B.11, 14C.10 and 14D.9 of the AML/CFT and TFs for FIs Policy Document.

[7] For the money services business sector, FIs shall also comply with IDV requirements for legal persons and the authorised person under the AML/CFT and TFS for FIs (Supplementary Document No. 1) - Money Services Business Sector Policy Document, as may be amended by the Bank from time to time.

behalf of the legal person; and

(iii) identification and reasonable measures for verification of beneficial owners[8] of the legal person.

G 8.9 In relation to paragraph 8.8(i), financial institutions may wish to undertake one or more verification methods to establish business legitimacy, such as but are not limited to those specified under Appendix 1.

S 8.10 For the money services business sector, in meeting requirements under paragraph 8.8 (i) - (ii) and paragraph 8.9 of this policy document, money services businesses [9] shall also comply with IDV requirements for legal persons, i.e. corporate customers and the authorised person under the AML/CFT and TFS for FIs (Supplementary Document No. 1) - Money Services Business Sector Policy Document, as may be amended by the Bank from time to time. For the avoidance of doubt, the more stringent requirements specified in the aforementioned policy document shall apply to money services businesses.

S 8.11 In relation to paragraph 8.8(ii), where the identification and verification of the authorised person is conducted via electronic means, a financial institution shall ensure that-

(i) electronic communication or documents that capture collective decision making by the directors of the legal person (e.g. digital forms of Directors Resolution or Letter of Authority) to appoint the authorised person and establish business relations are maintained in accordance with relevant record keeping requirements as specified under paragraph 24 of the AML/CFT and TFS for FIs Policy Document;

(ii) such electronic means adopted to identify and verify the authorised person are within the legal person's constitution or any other document which sets out the powers of the legal person; and

(iii) the authorised person is identified and verified through e-KYC as an individual, having due regard to the measures listed under paragraph 8.6 of this policy document.

G 8.12 In respect of paragraph 8.11 (i), such electronic means to capture collective decision making by the directors of the legal person on the appointment of the authorised person may include but are not limited to the following-

(i) utilising electronic technologies that identify and verify the directors, and subsequently capture evidence of directors' consent (e.g. audited/circulated email trails, providing agreement or disagreement through personal secure authentication links for directors to consent, video-conferencing to verify consent); and/or

(ii) using third parties (e.g. Digital Company Secretaries) that may provide confirmation on the legitimacy of relevant evidence such as the Directors

[8] As required under paragraphs 14A.9.6, 14B.11.12, 14C.10.7 and 14D.9.6 of the AML/CFT and TFS for FIs policy document.

[9] Refers to reporting institutions licensed under the MSBA which carry on remittance and/or money-changing business using non- Face to Face onboarding verification process for legal persons.

Resolution or Letter of Authority.

S 8.13 A financial institution shall undertake their own risk assessment to clearly define parameters for classifying potential legal persons (e.g. higher risk) that are not allowed to establish business relations through e-KYC.

Question 3:
In relation to e-KYC for legal persons, please provide feedback on the following-

a) Do you or your company anticipate any challenges in developing e-KYC solutions for legal persons, in view of the proposed requirements and guidance? Are there any additional key considerations you would like to suggest?
b) What are some other possible electronic means you would like to suggest of capturing collective decision making by the directors of a legal person on the appointment of an authorised person?
c) Apart from conducting CDD via online searches of databases, are there other effective means of identifying and verifying beneficial owners (BOs)?
d) Apart from the verification methods listed in Appendix 1, are there any other methods which may be relevant to include?

Ensuring effective e-KYC implementation

G 8.14 e-KYC solutions may utilise artificial intelligence, machine learning or other forms of predictive algorithms to ensure accurate identification and verification. This may result in automation of the decision-making process for customer on-boarding, thus reducing the need for human intervention.

S 8.15 Where the decision to verify a customer's identity through e-KYC is automated with the use of artificial intelligence, machine learning or other forms of predictive algorithms, whether in whole or in part, a financial institution shall ensure that the e-KYC solution is continuously capable of accurately distinguishing between genuine and non-genuine cases of customer on-boarding.

S 8.16 For the purposes of paragraph 8.15, in ensuring accuracy of the e-KYC solution, a financial institution shall take steps to minimise the False Acceptance Rates (FAR), defined as $\frac{False\ Positive}{(False\ Positive + True\ Negative)}\ x\ 100$. In measuring and assessing the FAR, a financial institution shall observe the considerations and requirements listed in Appendix 2[10].

[10] For avoidance of doubt, requirements for FAR within this policy document do not apply to e-KYC solutions where verification of customer identity is automated without the use of artificial intelligence, machine learning or other similar forms of predictive algorithms.

Question 4:

a) In view of improvements observed in the accuracy of e-KYC technology and rise of more sophisticated tools used for fraud detection purposes (e.g. deepfakes), do you think FAR should still be used as an accuracy measurement tool to trigger internal review?

b) If no, what are the limitations of maintaining the FAR as a tool to measure accuracy? Are there better ways to measure effectiveness and accuracy of e-KYC solutions?

c) Please provide feedback on challenges and observations of FAR performance during implementation (e.g. at different stages of implementation), if any.

Reliance on human representatives

G 8.17 Notwithstanding paragraphs 8.14 to 8.16, a financial institution may also perform e-KYC where identification and verification is conducted solely by a human representative. This includes cases where the decision to verify a customer is conducted by a financial institution representative, intermediary or insurance agent, with the assistance of electronic means such as video calls using mobile devices.

G 8.18 In contrast with e-KYC solutions under paragraphs 8.14 to 8.16 that utilise both machine and human [11] capabilities, e-KYC performed solely by a human representative through electronic means may involve a lower level of identity assurance due to human limitations and thus may not be suitable for all circumstances.

S 8.19 Where the decision to verify a customer's identity through e-KYC is conducted solely by a human representative, a financial institution shall give due regard to situations where there is potential for higher risk of misidentification and establish necessary safeguards to address this risk.

Addressing ongoing vulnerabilities

S 8.20 A financial institution shall continuously identify and address potential vulnerabilities[12] in the e-KYC solution.

S 8.21 In respect of paragraph 8.20, actions to address potential vulnerabilities shall include conducting reviews on the e-KYC solution and, where applicable, submitting periodical feedback to technology providers with the aim of improving effectiveness of the underlying technology used for customer identification and verification.

[11] By virtue of audits that are conducted under Appendix 2.

[12] Potential vulnerabilities include exposures to IT, operational and ML/TF related risks.

Additional safeguards to facilitate deployment

G 8.22 The availability of data is an important factor in the effectiveness of e-KYC solutions for identification and verification.

S 8.23 Where there are limited data points to determine accuracy of the e-KYC solution in the initial deployment stage, a financial institution shall consider additional safeguards, particularly for products that pose higher risks arising from inaccurate identification.

S 8.24 To facilitate deployment of e-KYC solutions for products with higher risks arising from inaccurate identification, a financial institution shall observe the considerations and safeguards specified in Appendix 3. This list may be updated as and when there are developments in the e-KYC landscape, including availability of better performance data on the effectiveness of specific e-KYC methods.

Question 5:

a) Appendix 3 provides a list of additional verification measures and ringfencing parameters which may be adopted to facilitate e-KYC for 'new-to-market' customers. Apart from said measures, are there other measures that can facilitate e-KYC for the unbanked, which are equally or more effective than the credit transfer safeguard? If yes, please indicate and elaborate.

b) What would be the challenges or implications, if any, in maintaining the credit transfer safeguard for banked customers only? Please provide feedback on this area.

9 Reporting requirements

S 9.1 In monitoring the effectiveness and accuracy of e-KYC solutions utilising artificial intelligence, machine learning or other forms of predictive algorithms, a financial institution shall maintain a record of the performance of the e-KYC solution segregated on a monthly basis in accordance with the reporting template specified in Appendix 4.

S 9.2 The records required to be maintained under this policy document shall be made readily available for review by the Bank.

S 9.3 A financial institution shall submit the record in relation to paragraph 9.1 via the STATsmart online submission system.

S 9.4 A financial institution shall submit the record in relation to paragraph 9.1 on a half-yearly basis according to the following arrangement-

(i) For the period of January to June of each year, the record shall be submitted no later than 4 August of the same year; and

(ii) For the period of July to December each year, the record shall be

submitted no later than 4 February the following year.

S 9.5 In respect of paragraph 9.4, in the event that the deadline falls on a non-working day, the deadline will be extended to the next immediate working day, unless specifically informed by the Bank in writing on the revised deadline.

PART C REGULATORY PROCESS

10 Notification for licensed persons and prescribed development financial institutions

S 10.1 Subject to paragraphs 8.1 and 8.2, where a licensed person[13] or a prescribed development financial institution[14] meets the requirements stipulated in this policy document and intends to implement an e-KYC solution described in paragraph 8.7 for the first time[15], a complete list of information as set out in Appendix 5 shall be submitted to the Bank.

S 10.2 In respect of paragraph 10.1, a licensed person or a prescribed development financial institution may proceed to implement and utilise the e-KYC solution after 14 working days from the date of receipt by the relevant Departments of the Bank of the complete submission of information set out in Appendix 4. The submission of information to the Bank shall be made to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan or Jabatan Penyeliaan Insurans dan Takaful, as the case may be and shall be signed off by the Chief Executive Officer, Chief Risk Officer or Chief Operating Officer who has the responsibility to ensure that the information submitted pursuant to this paragraph is complete and accurate.

G 10.3 In respect of paragraph 10.1, where a licensed person or a prescribed development financial institution intends to implement the e-KYC solution for the first time and the product to be offered qualifies as a new product as defined under the Introduction of New Products policy document[16], the information required under the aforementioned policy document and this policy document may be submitted together to the Bank.

S 10.4 Prior to submitting the information required in paragraph 10.1, a licensed person or a prescribed development financial institution, where relevant, shall ensure compliance to the Bank's RMiT and Outsourcing policy documents.

---

[13] As defined under the FSA or IFSA.

[14] As defined under the DFIA. This excludes cases where a prescribed development financial institution licensed under the MSBA intends to implement e-KYC for remittance services.

[15] For avoidance of doubt, this requirement also applies to a financial institution implementing e-KYC in the following situations for the first time: (i) e-KYC for legal persons; and/or (ii) e-KYC for higher risk products without a credit transfer safeguard.

[16] Or in the case of life insurers and family takaful operators, the Introduction of New Products by Insurers and Takaful Operators policy document.

11 Approval for licensed money-changing operators, licensed remittance service providers, approved non-bank issuers of designated payment instruments and approved non-bank issuers of designated Islamic payment instruments

S 11.1 Subject to paragraphs 8.1 and 8.2 and as required under the AML/CFT and TFS for FIs policy document, licensed money-changing operators, licensed remittance service providers[17], approved non-bank issuers of designated payment instruments and approved non-bank issuers of designated Islamic payment instruments shall obtain a written approval from Jabatan Pemantauan Perkhidmatan Pembayaran prior to implementing e-KYC.

S 11.2 In respect of paragraph, 11.1, application for approval shall include a complete list of information as set out in Appendix 5.

12 Enforcement

S 12.1 Where the Bank deems that the requirements in this document have not been complied with, the Bank may take appropriate enforcement action against the financial institution, including the directors, officers and employees with any provision marked as "S" in this document or direct a financial institution to-

(i) undertake corrective action to address any identified shortcomings; and/or

(ii) suspend or discontinue implementation of e-KYC.

[17] This includes cases where a prescribed development financial institution licensed to conduct remittance service under the Money Services Business Act 2011 (MSBA) intends to implement e-KYC for remittance services.

APPENDICES

Appendix 1: Examples of verification methods to establish business legitimacy

1. In developing e-KYC methods for legal persons, a financial institution may wish to consider undertaking at least one or more verification methods that is relevant to the nature or business model of the legal person. This aims to provide heightened assurance on the legitimacy of the legal person's business.

2. Such verification measures may include but are not limited to the following-

   (i) make unannounced video calls to the CEO, directors, or authorised person assigned to the legal person. During the video call, a financial institution may request the person to show proof of business existence such as signboard or inventories (if any);

   (ii) identify and verify the location of legal person to ensure that the location matches the registered or business address of the legal person. A financial institution may also verify location of the CEO, directors, or authorised person during the video call;

   (iii) verify the legal person's information against a database maintained by credible independent sources such as relevant regulatory authorities, government agencies or associations of the regulated sectors. A financial institution may also request for the legal person's active bank account or audited financial statement as proof of on-going business activity; and/or

   (iv) any other credible verification methods as proposed by financial institutions to the Bank.

Question 6:
In relation the verification measures listed in paragraph 2 of this Appendix, the Bank welcomes feedback on the listed verification measures, potential implementation challenges, if any, and other methods that may be similarly effective.

Appendix 2: False Acceptance Rate

1. In measuring the accuracy and effectiveness of e-KYC solutions, the FAR may be considered a useful measurement as it captures the capability of the solution to identify non-genuine identification and verification cases. Generally, a lower FAR indicates that the e-KYC solution has correctly identified non-genuine or fraudulent identification and verification attempts on a regular basis.

2. FAR shall be measured based on the number of complete[18] identification and verification cases processed under e-KYC.

3. In determining FAR, a financial institution shall conduct audits to classify identification and verification cases into genuine and non-genuine cases. Where it is not feasible for a financial institution to audit every identification and verification case facilitated through e-KYC, a financial institution may adopt a sampling approach. In doing so, a financial institution shall ensure that the data used to determine FAR is random, unbiased and representative of the customer base.

4. In respect of paragraph 3 of this Appendix, a financial institution shall conduct audits on current month e-KYC cases by the last day of the following month (e.g. January cases to be audited by the last day of February) for the first six months of e-KYC implementation. After the first six months of e-KYC implementation, a financial institution shall conduct the audits no less than once every quarter, where current quarter e-KYC cases shall be conducted by the last day of the first month of the following quarter (e.g. first quarter cases to be audited by the last day of April).

5. A financial institution shall aim to ensure that the overall FAR for the e-KYC solution does not exceed 5% and take steps to continuously improve the e-KC solution and thereby reduce the overall FAR. The level of FAR should also take into consideration the number of identification and verification cases, and the risks associated with inaccurate identification for a particular product or service offered through e-KYC.

6. Generally, for e-KYC solutions leveraging the use of artificial intelligence, FAR should reduce with the increase in identification and verification cases processed.

7. Where the overall FAR is measured to be more than 5% for any three months within a six-month period, a financial institution shall notify Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan, Jabatan Penyeliaan Insurans dan Takaful or Jabatan Pemantauan Pembayaran.

[18] A complete identification and verification case processed under e-KYC is defined as a case where the customer has completed only the e-KYC checks as described in paragraph 2 of Appendix 3. This includes cases where e-KYC for individuals related to legal persons are implemented. This does not include other steps in the e-KYC process (e.g. credit transfer).

8. In respect of paragraph 7 of this Appendix, the notification to the Bank shall include the following-
   (i) an assessment on the current performance of the e-KYC solution, including reasons for the observed level of FAR;
   (ii) proposed action to reduce the FAR going forward; and
   (iii) proposed mitigating actions or additional controls to safeguard the effectiveness of the e-KYC process.

9. In respect of paragraph 8(iii) of this Appendix, the mitigating actions and/or additional controls may include but are not limited to the following-
   (i) enhanced monitoring of customers identified and verified through e-KYC; and/or
   (ii) conducting audits on e-KYC cases prior to opening an account

Appendix 3: e-KYC safeguards to be adopted by financial institutions offering higher risk financial products

1. List of products[19] subjected to e-KYC safeguards-
   (i) current account;
   (ii) savings account; and
   (iii) unrestricted investment account with funds placement and withdrawal flexibilities as well as funds transfer features.

e-KYC for individuals with credit transfer for higher risk products

2. A financial institution offering the financial products in paragraph 1 of this Appendix through e-KYC for the purpose of customer identification and verification shall at minimum-
   (i) verify the customer against a government issued ID by utilising biometric technology;
   (ii) ensure that the government issued ID used to support e-KYC customer verification is authentic by utilising appropriate fraud detection mechanisms;
   (iii) ensure the customer is a live subject and not an impersonator (e.g. use of photos, videos, facial masks) by utilising liveness detection; and
   (iv) undertake measures to demonstrate that the customer has an existing bank account with another licensed person and is able to access said bank account. This may be achieved through requiring the customer to perform a credit transfer or to verify an amount transferred to the said bank account.

3. In respect of paragraph 2(iv) of this Appendix, a financial institution shall ensure that the customer details (i.e. name or identity document number) obtained in relation to the bank account with another licensed person is consistent with the details supplied by the customer.

e-KYC for individuals without credit transfer for higher risk products

4. The requirement in paragraph 2(iv) of this Appendix does not apply where an individual customer does not have any existing bank account with another licensed person and thus is unable to perform the credit transfer step. In lieu of the credit transfer safeguard, a financial institution intending to offer the products listed in this Appendix to individual customers shall ensure to-
   (i) have in place sufficient controls based on internal assessment of risk arising from offering the product without the credit transfer step;
   (ii) be able to demonstrate that their e-KYC solution remains effective and secure; and

[19] Requirements in this Appendix apply to existing individual customers of a financial institution that do not have any of the products listed in paragraph 1 of this Appendix and is intending to apply for one through e-KYC. For avoidance of doubt, requirements in this Appendix does not apply to legal persons identified and verified through e-KYC.

(iii) consider building in additional verification measures and ringfencing parameters [20] to establish higher assurance levels and limit risk exposure.

5. In respect of paragraph 4 of this Appendix, a financial institution shall take reasonable measures to verify whether the individual customer has an existing bank account with another licensed person. This may include but are not limited to the following measures-

(i) initiating an instant transfer (i.e. DuitNow) query via the customer's mobile phone number or IC number and verifying whether information on the query matches the customer's personal details or otherwise;

(ii) presenting a declaration form for the customer to confirm that the customer does not have an existing bank account with another licensed person.

Question 7:
In relation to paragraphs 4 and 5, the Bank welcomes feedback on other methods that can explored to verify whether an individual customer has an existing bank account, potential implementation challenges, if any and corresponding alternative solutions.

6. In respect of paragraph 4(iii) of this Appendix, examples of additional verification measures and ringfencing parameters that may be undertaken and built into the e-KYC process to provide a higher level of assurance for customers in absence of a credit transfer include but are not limited to-

(i) limiting product functionality at the initial period of account opening (e.g. lower account limits, no wire transfer);

(ii) conducting audits for on-boarding cases prior to granting access to account;

(iii) un-announced telephone or video calls to the customer;

(iv) require customers to complete online questionnaires for account opening applications that require a wide range of information, which can be verified by a third party;

(v) confirming the customer's identity during physical delivery of bank cards;

(vi) introducing specific transaction monitoring tools and stricter on-going due diligence triggers for accounts opened through e-KYC; and

(vii) conducting randomised audits on e-KYC cases post on-boarding.

7. Where a financial institution intends to adopt an e-KYC process without credit transfer for higher risk products for the first time, the financial institution shall comply with notification requirements in paragraph 10.1 of this policy document.

[20] E.g. Time-bound limitations, control group limitations, product functionality and phasing limitations.

Appendix 4: Reporting Template

1. The performance data below shall be recorded when reporting e-KYC identification and verification cases performed by a financial institution[21]-

	(Year)			
Data	**January**	**…**	**June**	**Total**
Total identification and verification cases performed				
Total identification and verification cases that were accepted by solution				
Total sample size of identification and verification cases audited				
True Positive (no. of cases)				
True Negative (no. of cases)				
False Positive (no. of cases)				
False Negative (no. of cases)				
False Acceptance Rate (%)				
False Rejection Rate (%), defined as $\frac{No.\ of\ False\ Negatives}{(No.\ of\ False\ Negatives + No.\ of\ True\ Positives)}\ x\ 100$				

[21] For avoidance of doubt, the term "cases" in the table under paragraph 1 of this Appendix refer to complete identification and verification cases as defined in footnote 18 of Appendix 2.

2. A robust e-KYC solution may consist of a series of e-KYC checks (e.g. document authenticity and biometric checks as outlined in paragraph 8.6) in identifying and verifying a customer. Where a financial institution utilises a series of e-KYC checks in the solution, the performance data below shall be recorded for each e-KYC check-

	(Year)			
Type of e-KYC checks	**January**	**…**	**June**	**Total**
Document authenticity, segregated by-				
a) *MyKad*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
b) *Passport*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
c) *Other official identity documents*				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				
Biometric matching				
True Positive				
True Negative				
False Positive				
False Negative				
FAR (%)				

3. Other relevant metrics to be reported-

Average time taken for completion of e-KYC process[22] Average time taken from start of application to- (i) completion of application (minutes); (ii) account opening (minutes); and (iii) account activation (hours).	

[22] Items (ii) and (iii) under paragraph 3 of this Appendix are not applicable to life insurers and family takaful operators.

Appendix 5: Information Required for Submission

1. A detailed product description, including its features, structure and target market or customers. Product illustrations shall also be included where appropriate.

2. Sample product term sheet.

3. Detailed information on the key features of the e-KYC solution. This may include types of checks, customer information captured and any other material information.

4. A written assessment on the effectiveness of the e-KYC solution. The written assessment may consider accuracy of technology functions, types of checks included and any other relevant information that may attest for the effectiveness of the underlying technology. Where relevant, the assessment should include FAR results gathered from conducting negative testing of fraudulent scenarios[23] on the e-KYC solution. Other relevant information supporting the written assessment such as independent assurance, review or certification may also be considered for this purpose.

5. In the case where a financial institution chooses to engage a technology provider, the assessment to demonstrate effectiveness of the e-KYC solution may include the technology provider's company background and track record in other jurisdictions or industries.

6. Description of key inherent risks of the e-KYC solution and arrangements in place to manage those risks. Where a financial institution deems it necessary, plans for implementation of enhanced monitoring and reporting mechanisms to identify potential ML/TF activities should also be included in the description.

7. Detailed end-to-end process flow of the e-KYC solution. This may include but is not limited to an illustration of the customer journey and decision-making process from start of application to account opening.

8. Any other relevant information to demonstrate a financial institution's ability to comply with the standards in this document and any other related policy documents issued by the Bank, including, where applicable-
   (i) RMiT policy document; and
   (ii) Outsourcing policy document.

9. Any additional documents or information as may be specified by the Bank.

[23] Negative testing may include testing the e-KYC solution against photocopied ICs, deepfake technology or any other method which may spoof the e-KYC solution into accepting an inaccurate on-boarding attempt.