BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Electronic Know-Your-Customer (e-KYC)

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

Issued on: 30 June 2020 BNM/RH/PD 030-10

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 The digitalisation of identification and verification processes is an important enabler to increase the convenience and reach, as well as lower the costs of financial services. A key aspect of digitalisation entails the delivery of end-to-end financial solutions through online and mobile channels, supported by the adoption of financial technology.

1.2 The digitalisation process, if not effectively managed, can become a source of risk to a financial institution and can undermine the integrity of financial transactions. The Bank expects the outcome of e-KYC technology adoption in the financial sector to include uncompromised accuracy in customer identification and verification, along with an ongoing assessment of the robustness of the technology application.

1.3 This policy 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 identification and verification of individuals. 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 Counter Financing of Terrorism (AML/CFT) control measures.

2 Applicability

2.1 This policy document is applicable to all financial institutions as defined in paragraph 5.2.

2.2 This policy document shall not apply to agent banking channels governed under the policy document on Agent Banking 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 2001 Act (AMLA).

4 Effective date

4.1 This policy document comes into effect on 30 June 2020.

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 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.

"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-
(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.

"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, "customer" refers to a person for whom the licensee undertakes or intends to undertake business transactions.

"electronic Know-Your-Customer (e-KYC)" means establishing business relationships and conducting customer due diligence (CDD) [1] 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.

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 and guidelines issued by the Bank, in particular-

(i) Anti-Money Laundering, Counter Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs) dated 1 January 2020;

[1] This includes cases of simplified CDD and CDD on a beneficiary as specified under the AML/CFT and TFS for FIs policy document.

(ii) Risk Management in Technology (RMiT) dated 19 June 2020;
(iii) Outsourcing dated 23 October 2019;
(iv) Management of Customer Information and Permitted Disclosures dated 17 October 2017;
(v) Introduction of New Products dated 7 March 2014; and
(vi) Introduction of New Products by Insurers and Takaful Operators dated 15 May 2015.

PART B POLICY REQUIREMENTS

7 e-KYC implementation

Roles and responsibilities of the Board

S 7.1 A financial institution shall obtain Board approval on the overall risk appetite and internal framework governing the implementation of e-KYC. 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 7.2 The Board 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, customer information, human capital, information technology (IT) and money laundering and terrorism financing (ML/TF) risks.

Identification and verification through e-KYC

S 7.3 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.

S 7.4 A financial institution shall adopt an appropriate combination of authentication factors when establishing measures to verify the identity of a customer 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 7.5 In respect of paragraph 7.4, a financial institution should have regard to the three basic authentication factors, namely, something the customer possesses (e.g. identity card, registered mobile number), something the customer knows (e.g. PIN, personal information) and 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.

G 7.6 In identifying and verifying a customer's identity through e-KYC as required by the policy document on AML/CFT and TFS for FIs, 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 used 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, facial masks) by utilising liveness detection.

Use of artificial intelligence, machine learning or other forms of predictive algorithms

G 7.7 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 identification and verification, thus reducing the need for human intervention.

S 7.8 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 capable of accurately distinguishing between genuine and non-genuine cases of customer identification and verification.

S 7.9 For the purposes of paragraph 7.8, in ensuring accuracy of the e-KYC solution, a financial institution shall take steps to minimise the overall False Acceptance Rates (FAR), defined as $\frac{No.\ of\ False\ Positives}{(No.\ of\ False\ Positives + No.\ of\ True\ Negatives)}\ x\ 100$. In measuring and assessing the FAR, a financial institution shall observe the considerations and requirements listed in Appendix 1[2].

Reliance on human representatives

G 7.10 Notwithstanding paragraphs 7.7 to 7.9, 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 7.11 In contrast with e-KYC solutions under paragraphs 7.7 to 7.9 that utilise both machine and human[3] 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 7.12 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

[2] For avoidance of doubt, requirements for FAR within this policy document do not apply to e-KYC solutions where the decision to verify a customer's identity is (i) automated without the use of artificial intelligence, machine learning or other similar forms of predictive algorithms; or (ii) conducted solely by a human representative, as described in paragraph 7.10.

[3] By virtue of audits that are conducted under Appendix 1.

situations where there is potential for higher risk of misidentification and establish necessary safeguards to address this risk.

Addressing ongoing vulnerabilities

S 7.13 A financial institution shall continuously identify and address potential vulnerabilities[4] in the e-KYC solution.

S 7.14 In respect of paragraph 7.13, 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.

Additional safeguards to facilitate deployment

G 7.15 The availability of data is an important factor in the effectiveness of e-KYC solutions for identification and verification.

S 7.16 Where there are limited data points to determine accuracy of the e-KYC solution in the initial deployment stage, a financial institution shall establish additional safeguards, particularly for products that pose higher risks arising from inaccurate identification.

S 7.17 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 2. 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.

8 Reporting requirements

S 8.1 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 3.

S 8.2 The records required to be maintained under this policy document shall be made readily available for review by the Bank.

S 8.3 A financial institution shall submit the record in relation to paragraph 8.1 in accordance with instructions set out in Appendix 5 via the Integrated

[4] Potential vulnerabilities include IT, operational, human capital, customer information and ML/TF related risks.

Submission Platform, a web-based application set up by the Bank.

S 8.4 A financial institution shall submit the record in relation to paragraph 8.1 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 of each year, the record shall be submitted no later than 4 February of the following year.

S 8.5 In respect of paragraph 8.4, 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

9 Notification for licensed persons and prescribed development financial institutions

S 9.1 Subject to paragraphs 7.1 and 7.2, where a licensed person[5] or a prescribed development financial institution[6] meets the requirements stipulated in this policy document and intends to implement an e-KYC solution described in paragraph 7.7 for the first time, a complete list of information as set out in Appendix 4 shall be submitted to the Bank.

S 9.2 In respect of paragraph 9.1, 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 9.3 In respect of paragraph 9.1, 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[7], the information required under the aforementioned policy document and this policy document may be submitted together to the Bank.

S 9.4 Prior to submitting the information required in paragraph 9.1, a licensed person or a prescribed development financial institution, where relevant, shall ensure compliance to the Bank's RMiT and Outsourcing policy documents.

10 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 10.1 Subject to paragraphs 7.1 and 7.2 and as required under the policy document on AML/CFT and TFS for FIs, licensed money-changing operators, licensed remittance service providers[8], approved non-bank issuers of designated

[5] As defined under the FSA or IFSA.
[6] 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.
[7] Or in the case of life insurers and family takaful operators, the Introduction of New Products by Insurers and Takaful Operators policy document.
[8] This includes cases where a prescribed development financial institution licensed to conduct remittance service under the MSBA intends to implement e-KYC for remittance services.

payment instruments or approved non-bank issuers of designated Islamic payment instruments shall obtain a written approval from the Bank prior to implementing e-KYC.

S 10.2 In respect of paragraph 10.1, an application for approval shall include a complete list of information as set out in Appendix 4.

11 Enforcement

S 11.1 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.

APPENDICES

Appendix 1: 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[9] 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%. However, 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, Jabatan Pengawalan Perniagaan Perkhidmatan Wang or

[9] 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 does not include other steps in the e-KYC processs (e.g. credit transfer).

Jabatan Pemantauan Pembayaran, as the case may be, in writing. The notification shall be made within seven working days upon the completion of the latest audit and detection of the aforementioned FAR scenario.

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

1. List of products subjected to e-KYC safeguards-
   (i) current account;
   (ii) savings account; and
   (iii) unrestricted investment account[10] with funds placement and withdrawal flexibilities as well as funds transfer features.

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-[11]
   (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.

[10] Refers to unrestricted investment accounts as defined in the policy document on Investment Account dated 14 March 2014.

[11] Requirements in this Appendix apply to existing 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.

Appendix 3: Reporting template

1. The performance data below shall be recorded when reporting e-KYC identification and verification cases performed by a financial institution-[12]

	(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 $\frac{No.\ of\ False\ Negatives}{(No.\ of\ False\ Negatives + No.\ of\ True\ Positives)}\ x\ 100$				

[12] For the 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 9 of Appendix 1.

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 7.6) 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.[13] Average time taken from start of application to- (i) completion of application (minutes); (ii) account opening (minutes); and (iii) account activation (hours).	

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

Appendix 4: 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, where relevant, types of checks, technology used, 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 technology functions, types of checks included and any other relevant information that may attest for the effectiveness of the e-KYC solution. Where a financial institution chooses to engage a technology provider, this may include company background and track record in other jurisdictions or industries.

5. 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.

6. 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.

7. 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.

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

Appendix 5: Submission instructions

PART A SPECIFIC INSTRUCTIONS

1. The completed e-KYC reporting template (Appendix 3) shall be submitted to the Bank via the Integrated Submission Platform (ISP) at https://statsmart.bnm.gov.my/statsmart/ in accordance with the guidance provided in parts B, C and D of this Appendix.

2. In submitting the required information, a financial institution shall observe the following steps-
   (i) a financial institution shall download the Excel template[14] via the ISP provided by the Bank;
   (ii) the financial institution shall not change the format and formula of the Excel template to avoid processing errors;
   (iii) all files submitted by the financial institution shall follow the File Naming Specification provided in Part C; and
   (iv) once the Excel template is completed offline and ready for submission, the financial institution shall upload the report via the ISP to transmit it online to the Bank.

3. Enquiries on reporting-related matters through telephone and emails shall be directed to respective officers at the general line 03-26988044-

Officers-in-charge	Extension	Email address
Jabatan Pengurusan Data dan Statistik (JPS)		jps_ips@bnm.gov.my
Puan Nur Farha Abdul Rahman	7819	
Puan Intan Sakinah Rustam	7808	
Puan Jenny Yan Chin Wai	7725	

[14] The reporting template shall be available and downloadable on the ISP by 1 November 2020.

PART B Guidelines to access the Integrated Submission Platform (ISP)

No.	Activity	By whom	Date
1.	(i) Connect to the BNM Production environment (via internet) to access STATsmart Portal https://statsmart.bnm.gov.my/statsmart (ii) For a new Reporting Entity[15] (RE) Submitter and RE Approver, please register via STATsmart Portal. (iii) Please be guided by Sections 3.0 of the Integrated Statistical System (ISS) User Manual on STATsmart for Reporting Entities (July 2018), provided in part D of this Appendix (hereafter **User Manual**). (iv) For first time login, RE Submitter and RE Approver are required to change the password immediately to activate the account after the registration is approved by RE Security Administrator (SA).	RE Submitter and RE Approver	Access request to designated Security Administrator to be completed by 31 December 2020.
2.	The appointed RE SA will be responsible to approve the registration of the new RE Submitter and RE Approver. Please be guided by Sections 4.0 of the **User Manual.**	RE Security Administrator (SA)	Upon registration of new RE Submitter & RE Approver
3.	Once the RE Submitter and RE Approver have been registered and activated in the STATsmart Portal, the appointed RE SA is required to login into the (ISP) via the 'Support' tab in STATsmart Portal to perform User Role Maintenance i.e. to assign RE Submitter and RE Approver to the relevant Submission Obligations as	R RE Security Administrator (SA)	1 November 2020 – 15 Jan 2021

[15] For purposes of this Appendix, a Reporting Entity (RE) has the same meaning as a financial institution as defined in paragraph 5.2 of this policy document.

	follows- Subject Area: **Financial Statistics** Sub-Subject Area: **Industry Specific Reporting** Submission Form Template: **e-KYC** Submission Obligation: **Electronic Know-Your-Customer** Please be guided by Section 9.1.4 of the User Manual.		
4.	RE Submitter and RE Approver may then proceed with submission process accordingly. Please be guided by Section 9.1.10 of the **User Manual.**	RE Submitter and RE Approver	15 January – 4 February 2021 and next submission deadlines

PART C File Naming Specifications

1. A RE shall name their e-KYC report in accordance with the following naming conventions-

Component	Data Type	Possible Values
Data Header	CHAR(4)	[**e-KYC**] Electronic Know-Your-Customer
FI Type	NUMERIC(2) / CHAR(3)	[**02**] Licensed bank [**03**] Licensed Islamic bank [**12**] Licensed investment bank [**33**] Prescribed development financial institution [**34**] Licensed insurance companies [**40**] Licensed Takaful operators [**38/39/58/71**] Approved non-bank issuers of designated payment instruments and designated Islamic payment instruments [**MSB**] Licensed money-changing operator and/or remittance service providers
FI ID For MSB: Entity Code/ Business Registration Number	NUMERIC(2)/ NUMERIC(3) For MSB: CHAR(7)	**01** to **99** **01** to **999** For MSB: **01** to **999999X**
Reporting Frequency	CHAR(2)	[**_1H**] Reporting Half-year *Example: Reporting date from 1 January to 30 June*
Reporting Year	CHAR(4)	[**2020**] YYYY *Example: Reporting year of 2020*
Form Version	CHAR(4)	[**V1.0**] VX.X *Form version of Reporting Template as issued by BNM*
Extension		**.xlsx**

2. Below are examples of the file naming conventions for e-KYC reports to be submitted to the Bank-

(a) Commercial Banks
e-KYC0217_1H2020V1.0.xlsx
Electronic Know-Your-Customer (e-KYC) report for reporting date 1 January 2020 to 30 June 2020 from CITIBANK BERHAD (format version 1.0).

(b) Islamic Banks
e-KYC0340_2H2020V1.0.xlsx
Electronic Know-Your-Customer (e-KYC) report for reporting date 1 July 2020 to 31 December 2020 from BANK ISLAM MALAYSIA BERHAD (format version 1.0).

(c) Investment Banks
e-KYC1215_2H2020V1.0.xlsx
Electronic Know-Your-Customer (e-KYC) report for reporting date 1 July 2020 to 31 December 2020 from KAF INVESTMENT BANK BERHAD (format version 1.0).

(d) Development Financial Institution
e-KYC3311_1H2021V1.0.xlsx
Electronic Know-Your-Customer (e-KYC) report for reporting date 1 January 2021 to 30 June 2021 from BANK KERJASAMA RAKYAT MALAYSIA BERHAD (format version 1.0).

(e) Insurance Companies
e-KYC34263_1H2021V1.0.xlsx
Electronic Know-Your-Customer (e-KYC) report for reporting date 1 January 2021 to 30 June 2021 from AIG MALAYSIA INSURANCE BERHAD (format version 1.0).

(f) Takaful and Retakaful Operators
e-KYC40605_1H2021V1.0.xlsx
Electronic Know-Your-Customer (e-KYC) report for reporting date 1 January 2021 to 30 June 2021 from TAKAFUL IKHLAS SDN. BHD (format version 1.0).

(g) Non-bank issuers of designated payment instruments and designated Islamic payment instruments
e-KYC3830_2H2021V1.0.xlsx
Electronic Know-Your-Customer (e-KYC) report for reporting date 1 July 2021 to 31 December 2021 from WIRECARD PAYMENT SOLUTIONS MALAYSIA SDN BHD (format version 1.0).

(h) Licensed money changer and/or remittance service providers
e-KYCMSB299861P_2H2021V1.0.xlsx

Electronic Know-Your-Customer report for reporting date 1 July 2021 to 31 December 2021 from ALIF MONEY CHANGER SDN. BHD (format version 1.0).

PART D User Manual

Note: Click on the icon to access the user manual.