Frequently Asked Questions (FAQs) and Answers
on the e-KYC Policy Document

FAQs issued on: 15 April 2024

Introduction

The FAQs are intended to provide clarification to financial institutions on common queries in relation to the enhanced policy document on "Electronic Know-Your-Customer (e-KYC)" dated 15 April 2024.

No.	Questions	Answers
General questions		
1.	Would procuring e-KYC services from a 3rd party technology vendor be deemed a material outsourcing arrangement?	Given the different permutations of e-KYC checks and arrangements, financial institutions are encouraged to self-assess the applicability of requirements stipulated under the Outsourcing policy document. In doing so, a financial institution must take into consideration the exact features of the e-KYC solution that will be implemented, including the nature of activities performed by the 3rd party, and the nature of any data shared[1]. Generally, arrangements where a significant portion of e-KYC services is operated by the 3rd party are likely to be considered as material outsourcing. Nevertheless, financial institutions are reminded that any arrangement with a 3rd party technology vendor should safeguard the confidentiality of customer information at all times, in line with requirements under the policy document on Management of Customer Information and Permitted Disclosures.
2.	In complying with the Risk Management in Technology (RMiT) policy document, would 3rd Party Attestation be required when financial institutions adopt e-KYC	When a financial institution adopts e-KYC for the first time, the notification requirements set forth in section 14 of RMiT policy document requires a financial institution to engage an independent external party to provide assurance that the financial institution has addressed the associated technology risks and

[1] For the avoidance of doubt, the Bank may determine that an arrangement is considered material pursuant to paragraph 12.5 of the Outsourcing policy document.

	services offered by a technology provider?	security controls relating to the introduction of new technology for e-banking, Internet insurance and Internet takaful. This is important to ensure the integrity of customer identity proofing and the security of online transaction authentication with the use of e-KYC technologies. The third-party attestation is not required for subsequent enhancement to the e-KYC solution, as listed in the Appendix 6 Positive List. Nevertheless, financial institutions must ensure the risks associated with the enhancement are identified and managed on on-going basis and the enhancement notified to the Bank. A financial institution which intends to adopt e-KYC services hosted in the public cloud must meet the regulatory process as set forth in section 15 of RMiT policy document. A financial institution must self-identify whether the cloud service is subject to the consultation or notification requirements, based on criteria outlined in paragraph 15.2 of RMiT policy document i.e., its track record in public cloud adoption and the readiness of its technology risk management framework to manage cloud risks.
3.	For e-KYC implementation, under which circumstances should the notification system prescribed under the e-KYC policy document be pursued? Subsequently, in which circumstances should the notification system prescribed under the Introduction of New Products[2]	When implementing an e-KYC solution as described under paragraph 8.19 of the e-KYC policy document for the first time, a licensed person or a prescribed development financial institution shall refer to both the process specified under the e-KYC policy document and the Introduction of New Products policy document. 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

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

	policy document be pursued instead?	qualifies as a new product as defined under the Introduction of New Products policy document[3], the information required under both policy documents may be submitted together to the Bank. Upon submission, the e-KYC solution may be implemented after 14 working days from the submission of information required to the Bank. Where a licensed person or a prescribed development financial institution is not implementing e-KYC 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, a licensed person or prescribed development financial institution shall refer to the requirements and processes specified under the Introduction of New Products policy document.
4.	Can customers be dismissed due to a false negative result which is due to limitations of financial institution's e-KYC system?	With respect to false negative results, financial institutions are reminded to not discriminate against customers affected by the financial institution's system limitations as means to ensure fair treatment of financial consumers. As such, false negative customers should not be immediately dismissed. Remedial actions should be considered where the customers can prove authenticity of their identification. These should include improvements to the e-KYC solution to reduce future occurrences of false negatives.
5.	With MyDigital ID implemented as the National Digital ID recently, can MyDigital ID fulfil some e-KYC requirements in this policy document?	The long-term view is that the use of a trusted, secure National Digital ID can significantly reduce the risk of identity theft and fraud, and as such would complement the existing e-KYC process. Nonetheless, it is important for financial institutions to establish full understanding of the level of security and assurance of the National Digital ID to satisfactorily assess whether it fulfils the identity verification needs of the financial sector. Where deemed appropriate, a financial institution may consider the use of a trusted and secure National

		Digital ID for identity verification purposes on top of existing processes. However, at this juncture this shall be subject to the financial institution's own risk assessment on whether the strength of the National Digital ID fulfils identity verification requirements under the e-KYC policy document and AML/CFT and TFS for FIs policy document, and where additional verification measures may be required. The Bank expects a further review of requirements in the e-KYC policy document in the near future to provide greater clarity on how the National Digital ID can complement the financial sector's e-KYC requirements.
e-KYC for the unbanked segment		
6.	How do financial institutions ensure that accounts opened without the credit transfer safeguard would not have fund transfer capabilities to accounts of the same name, as required under Appendix 4 of the e-KYC PD for customers without an existing bank account?	It is the responsibility of the financial institution offering products listed in paragraph 1 of Appendix 4 to the e-KYC PD to build in technical capabilities (e.g. name matching with fuzzy logic) that would enable the financial institution (as the fund transfer sending bank) to detect and block any fund transfer attempts to other accounts outside of the financial institution with the same customer's name. Nonetheless, these restrictions may be waived subject to conditions under paragraphs 7 and 8 of Appendix 4 which provide for circumstances where these restrictions need not apply.
7.	Can the use of a National Digital ID such as MyDigital ID waive ringfencing parameters and fund transfer limitations imposed on accounts opened by the unbanked segment?	As referred to in question 5 of this FAQ, the long-term view is that the use of a trusted, secure National Digital ID can significantly reduce the risk of identity theft and fraud, and as such potentially address the assurance level required for accounts opened by customers without an existing bank account. The Bank expects a further review of requirements in the e-KYC policy document in the near future – including those for the unbanked segment - to provide greater clarity on how the National Digital ID can complement the financial sector's e-KYC requirements.

Effectiveness of e-KYC solutions		
8.	What are the definitions of the terms used in relation to the enhanced sampling requirements?	Key terms are as follows: Sample size: Number of cases included in the study to represent total onboarding attempts via e-KYC. • Confidence level: Level of certainty that the result is true and reliable for the population. • Margin of error: Degree of error in results that differ from population value. • Population size: Total number of identification and verification cases performed via eKYC.
9.	How is the sample size computed?	1. Sample size equation $$Sample\ size = \frac{\frac{z^2 \times p(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p(1-p)}{e^2 \times N}\right)}$$ <u>Notes on fixed variables:</u> • Critical value of the normal distribution at 95% confidence level, z: 1.96 (95% confidence Level) • Margin error, e: 0.03 (3%) • Sample, portion, p: 0.5 • Onboarded customers, N: [Indicate Total number of identification and verification cases performed via eKYC] 2. Simplified formula $$Sample\ size = \frac{\frac{1.96^2 \times 0.5(1-0.5)}{0.03^2}}{1 + \left(\frac{1.96^2 \times 0.5(1-0.5)}{0.03^2 \times N}\right)}$$ $$Sample\ size = \frac{\frac{3.8416 \times 0.25}{0.0009}}{1 + \frac{3.8416 \times 0.25}{0.0009 \times N}} Sample\ size = \frac{1067.11}{1 + \frac{1067.11}{N}}$$ 3. Example of calculation with N = 2,000 onboarded customers through eKYC

		$$Sample\ size = \frac{1067.11}{1 + \frac{1067.11}{2000}}$$ $$Sample\ size = \frac{1067.111111}{1 + 0.533555555}$$ $$Sample\ size = 695.84\ (2\ d.p.) \approx 696$$ *Note: A sample size that meets a minimum 95% confidence level and 3% margin of error for a population size of 2,000 cases is approximately 696. This is the **minimum** sampling size expected to be conducted by financial instituitions. For rounding ease and higher levels of assurance, financial instituitions may wish to consider rounding up to at least 700 or above.* *Kindly refer to the sample size table as a guidance in Appendix I.*
10.	What if the total number of customers onboarded via e-KYC is less than (<) 400 per month?	Financial institutions shall conduct 100% sampling, i.e. all cases shall be sampled.
11.	Can financial institutions leverage on the technology provider (TP) to conduct this validation?	Yes, financial institutions may leverage on their TP to carry out the validation subject to adequate assessment of the TP's capacity and capabilities. However, any leveraging arrangement should be supplemented with periodic independent assurance checks by the financial institutions.
12.	Can TPs obtain certifications other than ISO standards specified in the e-KYC policy document?	Yes, TPs may opt to obtain any relevant ISO-equivalent certifications that are able to provide sufficient assurance on the three (3) e-KYC modules.
13.	Can a TP rely on a single assessment by an assessor, despite having multiple financial institutions subscribe to their solution?	Yes, TPs can rely on a single assessment even if the TP services multiple financial institutions. Further, financial institutions may consider any additional scope beyond the e-KYC policy document. We would also like to reiterate that the requirement to obtain assessment from a credible external independent assessor and relevant certifications for the three (3) e-KYC modules is applicable for the TP, not the financial institutions.

14.	Should the independent assessment of financial institution's own processes, procedures and controls be conducted by internal or external assessors?	The independent assessment may be performed by any independent party, at the financial institution's discretion.
15.	What are some examples of mitigating controls financial institutions can take where potential vulnerabilities in the e-KYC solution is detected?	Pursuant to paragraphs 8.29 and 8.30 of the e-KYC policy document, financial institutions are expected to identify triggers that should prompt an assessment of mitigation controls that may need to be introduced to manage the associated risks. This includes but is not limited to: (i) Risk considerations, trigger mechanisms and rectification measures as listed in Appendix 2 of the e-KYC policy document; and (ii) Where a notable number of common or repeated fraud cases (e.g. tampered IDs) were not successfully detected by the solution. Where vulnerabilities are detected, financial institutions may consider the following in addition to or in complement with those listed in Appendix 2 of the e-KYC policy document: (i) Full or heightened visual inspection sampling for all e-KYC applications before onboarding for a defined period; (ii) Back-testing of all customers onboarded through e-KYC for a defined period (e.g., past 3 to 6 months) using the enhanced e-KYC solution; and (iii) Developing a detailed work plan to address identified vulnerabilities. This plan should include interim milestones to indicate progress, such as the percentage of previous

		false positive cases that the solution can progressively reject.
16.	Are requirements on the technology provider and financial institutions referenced in paragraphs 8.22 to 8.25 of the e-KYC PD applicable to e-KYC solutions for both individuals and legal persons?	Yes, requirements paragraphs 8.22 to 8.25 of the e-KYC PD are applicable to e-KYC solutions for both individuals and businesses, particularly given that the authorised persons of the legal person would still be subject to identity verification requirements for individuals. As such, relevant requirements on the technology provider and financial institution would still apply.

Any refinements to the note will be updated by the Bank from time to time. Should you have additional queries related to the policy document, please submit your queries via any of the following means:

a) Mail : Director
Financial Development and Innovation Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur

b) Email : e-kycpolicy@bnm.gov.my

Appendix I: Sample Size Table

Population Size	Required Sample Size							
	Confidence Level = 95%				Confidence Level = 99%			
	Margin Error				Margin of Error			
	3.00%	2.50%	2.00%	1.00%	3.00%	2.50%	2.00%	1.00%
1 – 400	Minimum sample size shall be the entire population							
500	*341	*378	414	476	*394	422	447	486
600	*385	434	481	565	454	490	525	580
700	423	482	543	653	508	555	600	672
800	458	527	601	739	559	616	672	764
1,000	517	607	707	906	650	728	807	944
1,200	566	675	801	1,067	728	828	932	1,120
1,500	624	760	924	1,298	829	960	1103	1,377
2,000	697	870	1,092	1,656	962	1,143	1,351	1,786
2,500	749	952	1,225	1,984	1,064	1,290	1,562	2,174
3,500	818	1,069	1,425	2,566	1,211	1,513	1,902	2,892
5,000	880	1,176	1,623	3,289	1,351	1,738	2,272	3,845
7,500	935	1,276	1,819	4,212	1,484	1,966	2,677	5,171
10,000	965	1,333	1,937	4,900	1,561	2,103	2,939	6,247
25,000	1,024	1,448	2,191	6,939	1,722	2,407	3,567	9,991
50,000	1,045	1,491	2,292	8,057	1,784	2,528	3,841	12,486
75,000	1,053	1,506	2,327	8,514	1,805	2,572	3,942	13,620
100,000	1,056	1,514	2,345	8,763	1,816	2,594	3,995	14,267
250,000	1,063	1,528	2,379	9,249	1,836	2,635	4,093	15,603
500,000	1,065	1,532	2,390	9,424	1,843	2,649	4,126	16,106
1,000,000	1,066	1,535	2,396	9,513	1,846	2,656	4,144	16,369
2,500,000	1,067	1,536	2,399	9,568	1,848	2,660	4,154	16,531
10,000,000	1,067	1,537	2,401	9,595	1,849	2,662	4,159	16,614
100,000,000	1,068	1,537	2,401	9,604	1,849	2,663	4,161	16,639
300,000,000	1,068	1,537	2,401	9,604	1,849	2,663	4,161	16,641

Notes:

1. [ ] Refers to the **minimum** sample size financial institutions should adopt. For higher levels of assurance, financial institutions may wish to consider a higher Confidence Level and / or lower Margin of Error.
2. *Minimum sample size shall be at least 400.
3. Numbers are provided for illustrative / estimation purposes only. Financial institutions should determine the appropriate sample size required based on financial institutions' own calculation of the population size.