
**Effective date: 1 September 2022**

# GUIDELINES FOR BANKS AND FINANCIAL INSTITUTIONS
# GUIDELINES NO. FIU/G-1/2022/1

# GUIDELINES ON MEASURES FOR NON-FACE-TO-FACE CUSTOMER ONBOARDING AND ONGOING CUSTOMER DUE DILIGENCE

## 1. INTRODUCTION

1.1. These Guidelines are issued pursuant to section 32 of the Brunei Darussalam Central Bank Order, 2010 (BDCB Order).

1.2. These Guidelines are to be read alongside with the Notice No. FIU/N-1/2022/1 on Measures for Non-Face-To-Face Customer Onboarding and Ongoing Customer Due Diligence and should be read with:

1.2.1. Criminal Asset Recovery Order, 2012 (CARO);

1.2.2. Anti-Terrorism Order, 2011;

1.2.3. General Guidance Paper to Financial Institutions and Designated Non-Financial Businesses and Professions on Anti-Money Laundering and Combatting the Financing of Terrorism;

1.2.4. Guidance Paper to Financial Institutions on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Transaction Monitoring programme;

1.2.5. Standard Technology Risk Management Guidelines, Guidelines to Money Changer and Money Remittance Businesses, Guideline No. TRS/G-1/2019/1;

1.2.6. Guidelines on Technology Risk Management for Financial Institutions, Guidelines No. TRS/G-2/2022/1;

1.2.7. Guidelines on IT Third Party Risk Management for Financial Institutions, Guidelines No. TRS/G-3/2022/2;

1.2.8. Guidelines on Credit Risk Management for Banks, Guideline No. BU/G-1/2018/9;

1.2.9. Outsourcing Guidelines for Banks dated 7 September 2012;

1.2.10. Notice on Outsourcing for CMSLH, Notice No CMA/N-1/2020/15;

1.2.11. Guidelines on Minimum Standards for a Remittance System, Guideline No. SM/G-1/2020/1;

1.2.12. Guidelines for Remittance Collection Service, Guidelines No. SM/G-1/2021/3;

1.2.13. Notice on Application for Approval of Outsourcing Arrangement for Insurance Takaful, Notice No. TIU/N-1/2019/11;

1.2.14. Guidelines on Outsourcing Arrangement for Insurance Companies and Takaful Operators, Guidelines No. TIU/G-1/2019/10;

1.2.15. Guidelines on Risk Management and Internal Controls for Insurance Companies and Takaful operators, Guideline No TIU/G-3/2018/8;

1.2.16. Guidelines on Online Distribution for Insurance Companies and Takaful operators, Guideline No TIU/G-1/2020/11; and

1.2.17. Any other notices, directives or guidelines, which the Authority may issue from time to time.

1.3. These Guidelines are meant to assist Banks and Financial Institutions in setting up the minimum standards required when adopting E-KYC for use in the provision of its services, to ensure:

1.3.1. Requirements for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) relating to customer onboarding and ongoing customer due diligence are adhered to; and

1.3.2. A secure and robust system with the technology in place to withstand any form of cyber-attack which third parties may exploit to conduct fraudulent activities.

1.4. These Guidelines are not exhaustive and subject to revision from time to time as deemed necessary by the Authority.

1.5. These Guidelines take effect on 1 September 2022.

## 2. DEFINITIONS

2.1. For the purposes of these Guidelines, the following terms have the following meanings except where the context otherwise requires –

2.1.1. "Banks" have the same meaning as section 2, BDCB Order, 2010;

2.1.2. "biometric" refers to a biological aspect of a person's physical feature or characteristic which are unique and includes but not limited to facial features, fingerprints, retinal patterns or voice recognition;

2.1.3. "customer" has the same meaning as in section 2, CARO, 2012;

2.1.4. "E-KYC" or "E-KYC solution" refers to the use of electronic or digital means to verify the authenticity of a person in order to establish business relationships (i.e. onboarding) and conduct customer due diligence (CDD);

2.1.5. "E-KYC application" means the customer-facing application, user interface application and/or the Application Programming Interface (API) of the E-KYC solution;

2.1.6. "file checksum" means an alphanumeric value that uniquely represents the contents of a file, and is usually evaluated to verify the integrity of file to ensure two files are exact copies of each other;

2.1.7. "Financial Institutions" have the same meaning as section 2, BDCB Order, 2010;

2.1.8. "geolocation" refers to the identification of the geographic location of a user or device through various collected data such as network routing address or internal GPS coordinate information;

2.1.9. "optical character recognition" means the electronic conversion of typed, handwritten or printed text on an image into a digital and readable text;

2.1.10. "Turing test" means a test to identify between live human and robots. For example, the use of CAPTCHA to generate random code, analysis of the user online behavior, or specifying user to perform certain actions that can only be fully understood by humans; and

2.1.11. "vital signs" refers to measurements of the body's most basic functions, which includes body temperature, pulse or heart rate, respiration rate and blood pressure.

2.2. Any expression used in these Guidelines, except where expressly defined in these Guidelines or where the context requires otherwise, have the same meaning as in the BDCB Order, 2010.

## 3. GUIDE TO CONDITIONS OF E-KYC AUTHENTICATION PROCESS

3.1. In coming up with a sufficient E-KYC authentication process, Banks and Financial Institutions are expected to collect or utilise information and features that are uniquely attributed to each customer. Such information or features are classified into the following:

3.1.1 An item owned by the customer which may be a government-issued identification document, a mobile device, a password-generating hardware or unique token;

3.1.2 Any information only known to the customer which may be a password, PIN number or security questions; and

3.1.3 Characteristics that distinguishes a customer, i.e. biometric information.

3.2. Banks and Financial Institutions are expected to have technology in place to validate documents. For instance, fraud detection technology can determine whether or not the documents provided as proof of identity are authentic and not counterfeit or forged.

3.3. The technology used is expected to verify the existence of a customer in real-time. For instance, liveness detection technology can be used to scrutinise customers in real-time, determine customers are who they say they are and prevent impersonation attempts which may occur through use of images and recorded videos.

3.4. Banks and Financial Institutions are expected to adopt multiple factors of authentication in order for the overall authentication process to be more secure and robust. Solely validating on personal information commonly used for other types of verification may not be reliable for E-KYC, such as the government-issued identification number, date of birth and residential address.

## 4. GUIDE TO CUSTOMER ONBOARDING PROCESS WITH E-KYC

4.1. For verification purposes, Banks and Financial Institutions should be able to conduct the following:

4.1.1 Capturing customer identification by recording or sighting sufficient documents of the customer. For instance, this would involve the scanning of a customer's government-issued identification document, and to have the technology in place to assess whether or not the identification provided is authentic and the document provided is not forged; and

4.1.2 Utilise biometric technology to scrutinize customers virtually in real-time. For instance, Banks and Financial Institutions may request for an image or conduct a video call with a customer. This is to confirm the person uploading the document through the electronic device is indeed the customer and not another person attempting to provide false identification or impersonate another person.

4.2. In compliance with the record-keeping requirements, Banks and Financial Institutions should ensure the E-KYC is able to do the following:

4.2.1. Detect any records or information on the customer; and

4.2.2. Be accessible or linked to the customer database so as to assist Banks and Financial Institutions in conducting complete KYC/CDD requirements and risk categorisation of its customers.

## 5. GUIDE TO ONGOING CUSTOMER DUE DILIGENCE WITH E-KYC

5.1. Banks and Financial Institutions utilising E-KYC in conducting periodic reviews to previously obtained customer information should be able to specify certain information that can be obtained from or updated by the customers without the need for verification. For example:

5.1.1. Personal details of a customer such as the marital status, education or employment status and employer name;

5.1.2. Contact details such as a customer's home phone number, personal mobile phone number and e-mail address; and

5.1.3. Relevant addresses such as residential address, office address, home country address and mailing address.

## 6. TECHNOLOGY GUIDELINES ON E-KYC

6.1. The sensors and devices used for the E-KYC should not be from obsolete technology to ensure reliability and compatibility of biometric data, image, video and document taken. The sensors and devices should also be subjected to firmware or driver updates to prevent unwanted tampering. For example, a device check can be carried out on the E-KYC application to detect device firmware version and device model.

6.2. The image or document scanning, and text recognition (optical character recognition) components should duplicate the image or document with good quality, and convert the characters into text with good accuracy. It is recommended to perform test scanning of several samples to evaluate the accuracy.

6.3. To ensure timeliness and liveness of the biometric data, image and video taken for verification, the biometric, image and video should be taken during the time of registration such as verifying in real-time via video streaming or immediate verification as soon as a biometric data or image is taken.

6.4. The biometric data, image and video should be taken and stored in good quality to improve verification and prevent tampering. This can be done by evaluating file properties of the image or video such as image resolution, compression and file checksum.

6.5. To detect liveness during verification, the Banks and Financial Institutions should also evaluate other properties in real-time such as the network connection session, live streaming timestamp and IP geolocation information.

6.6. The liveness detection should be complemented with Turing test technique to detect that a user is human such as by requiring the user to perform random actions (i.e. head movement, reciting phrases, etc.) or measuring vital signs during verification.

6.7. Biometric data such as fingerprint or facial information is recommended to be compared with a verified biometric database. For example, the biometric data can be compared with biometric information from National Digital ID database or an equivalent. Alternatively, the biometric data can be compared with biometric information which had been previously obtained and stored such as on the database of Banks or Financial Institutions or on a customer's mobile device (e.g. Touch ID, Face ID).

6.8. All data used for E-KYC such as images, videos and biometric data should be securely stored only for the purpose of verification and should not be shared to other third-party unless consented by the customer. Banks and Financial Institutions should also observe personal data protection requirements set in BDCB's Guidelines on Technology Risk Management (Guidelines No. TRS/G-2/2022/1) and applicable laws which may be put into place.

6.9. Banks and Financial Institutions should ensure that they are able to access and analyse information required for the E-KYC testing such as application logs and audit trails. If

possible, the E-KYC application should be able to generate report with the required information. In addition, Banks and Financial Institutions should also monitor complaints from the customers relating to authentication errors and access fraud.

6.10. Banks and Financial Institutions should periodically review and assess the accuracy, effectiveness, relevance and unbiasedness of the E-KYC application especially if artificial intelligence is used.

6.11. Banks and Financial Institutions should perform periodic security assessment including vulnerability assessment, penetration testing and biometric presentation attack detection (e.g. based on ISO/IEC 30107-3:2017) on the E-KYC application to ensure security and reliability of the E-KYC application.

6.12. Banks and Financial Institutions are encouraged to adhere to the Guidelines on Technology Risk Management (TRS/G-2/2021/1). If the E-KYC solution is hosted or provided by a third-party, Banks and Financial Institutions should also observe the Guidelines on IT Third Party Risk Management (TRS/G-3/2021/2).

## 7. OTHER CONSIDERATIONS

7.1. Banks and Financial Institutions should ensure audit arrangements are in place to provide assurance on the effectiveness of the E-KYC solution, risk management and the robustness of security and internal controls. Such audit may be conducted by an appointed external auditor or the internal audit function that takes responsibility for the AML/CFT review within the Bank or Financial Institution's regular internal audit process.

7.2. In the event Banks and Financial Institutions intends to limit the use of E-KYC to a certain target audience, this can be done by limiting the IP address of the E-KYC or only enabling download of the application to the intended country or region.

7.3. In providing online and offline support to assist customers in resolving any issues within the E-KYC process, reliable modes of support such as a hotline number, live chat function and over the counter assistance may be used.

**MANAGING DIRECTOR**
**BRUNEI DARUSSALAM CENTRAL BANK**

Issue Date: 14 Zulhijjah 1443H / 14 July 2022M