৫০১৩০

বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট

১২ তলা, ২য় সংলগ্নী ভবন
বাংলাদেশ ব্যাংক, প্রধান কার্যালয়
মতিঝিল, ঢাকা-১০০০
বাংলাদেশ।

বিএফআইইউ সার্কুলার নং-২৯

তারিখ: ১৬ চৈত্র, ১৪৩২ বঙ্গাব্দ / ৩০ মার্চ ২০২৬ খ্রিস্টাব্দ

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা
বাংলাদেশে কার্যরত সকল বীমা প্রতিষ্ঠান, স্টক ডিলার ও স্টক ব্রোকার,
পোর্টফোলিও ম্যানেজার ও মার্চেন্ট ব্যাংকার, সিকিউরিটিজ কাস্টডিয়ান ও সম্পদ ব্যবস্থাপক প্রতিষ্ঠান।

প্রিয় মহোদয়,

মানি লন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে "Guidelines on Electronic Know Your Customer (e-KYC)" জারীকরণ প্রসঙ্গে।

মানিলন্ডারিং প্রতিরোধ আইন, ২০১২ (সংশোধিত ২০১৫), সন্ত্রাস বিরোধী আইন, ২০০৯ (সংশোধিত ২০১৩) ও আইন দুটির আওতায় জারীকৃত বিধিমালার সংশ্লিষ্ট বিধানাবলী পরিপালন এবং বাংলাদেশে কার্যরত বীমাকারী প্রতিষ্ঠান, স্টক ডিলার ও স্টক ব্রোকার, পোর্টফোলিও ম্যানেজার ও মার্চেন্ট ব্যাংকার, সিকিউরিটি কাস্টডিয়ান ও সম্পদ ব্যবস্থাপকের গ্রাহকের সাথে সম্পর্ক স্থাপন প্রক্রিয়া সহজীকরণের নিমিত্ত "Guidelines on Electronic Know Your Customer (e-KYC)" মানিলন্ডারিং প্রতিরোধ আইন, ২০১২ (সংশোধিত ২০১৫) এর ২৩(১)(ঘ) ও সন্ত্রাস বিরোধী আইন,২০০৯ (সংশোধিত ২০১৩) এর ১৫(১)(ঘ) ধারায় প্রদত্ত ক্ষমতাবলে জারি করা হলো।

বিএফআইইউ কর্তৃক জারিকৃত সার্কুলার নং-২৫, তারিখ ৮ জানুয়ারী ২০২০ এর নির্দেশনা এ সার্কুলার দ্বারা প্রতিস্থাপিত বলে গণ্য হবে।

সংযুক্তিঃ বর্ণনা মোতাবেক (৩৫ পৃষ্ঠা)।

আপনাদের বিশ্বস্ত,

(এ,কে,এম,গোলাম মাহমুদ)
পরিচালক(বিএফআইইউ)
ফোনঃ ৯৫৩০১৭০

প্রতিলিপি নং- বিএফআইইউ(পলিসি)-৩/২০২৬-৬৭৮ - ৬৯৫ তারিখ : উল্লিখিত

অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য প্রতিলিপি প্রেরণ করা হলো ঃ (জ্যেষ্ঠতার ক্রমানুযায়ী নয়)

১. সচিব, আর্থিক প্রতিষ্ঠান বিভাগ, অর্থ মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা।
২. চেয়ারম্যান, বাংলাদেশ সিকিউরিটিজ অ্যান্ড এক্সচেঞ্জ কমিশন, আগারগাঁও, ঢাকা। (সংশ্লিষ্ট সকলের জ্ঞাতার্থে বিতরণের/প্রেরণের অনুরোধসহ)।
৩. চেয়ারম্যান, বীমা উন্নয়ন ও নিয়ন্ত্রণ কর্তৃপক্ষ, ৩৭/এ দিলকুশা, মতিঝিল, ঢাকা। (সংশ্লিষ্ট সকলের জ্ঞাতার্থে বিতরণের/প্রেরণের অনুরোধসহ)।
৪. নির্বাহী পরিচালক/পরিচালক বাংলাদেশ ব্যাংক, মতিঝিল,
ঢাকা/চট্টগ্রাম/রাজশাহী/খুলনা/বগুড়া/সিলেট/বরিশাল/রংপুর/ময়মনসিংহ/ সদরঘাট,ঢাকা।
৫. নির্বাহী পরিচালক, বাংলাদেশ ব্যাংক ট্রেনিং একাডেমি, মিরপুর, ঢাকা।
৬. সকল বিভাগীয় প্রধান, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৭. গভর্নর মহোদয়ের ব্যক্তিগত কর্মকর্তা, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৮. ডেপুটি গভর্নর মহোদয়গণের ব্যক্তিগত কর্মকর্তা, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৯. চিফ ইকোনমিস্ট/নির্বাহী পরিচালক মহোদয়গণের ব্যক্তিগত কর্মকর্তা, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
১০. মহাপরিচালক, বাংলাদেশ ইনস্টিটিউট অব ব্যাংক ম্যানেজমেন্ট, মিরপুর, ঢাকা।
১১. পরিচালক, বাংলাদেশ ইনসিওরেন্স একাডেমি, ইনসিওরেন্স একাডেমি ভবন, ৫৩ মহাখালী বা/এ, ঢাকা।
১২. প্রেসিডেন্ট, বাংলাদেশ ইনস্যুরেন্স ফোরাম, ৩ দিলকুশা বা/এ (১৭ তলা), ঢাকা।
১৩. প্রেসিডেন্ট, বাংলাদেশ ইন্স্যুরেন্স এসোসিয়েশন, হোসেন টাওয়ার (১০ তলা), বক্স কালভার্ট রোড, নয়া পল্টন, ঢাকা।
১৪. ব্যবস্থাপনা পরিচালক, ইনভেস্টমেন্ট কর্পোরেশন অব বাংলাদেশ , শিল্প ব্যাংক ভবন, ৮ ডিআইটি এভিনিউ, ঢাকা।
১৫. চেয়ারম্যান/ব্যবস্থাপনা পরিচালক, ঢাকা স্টক এক্সচেঞ্জ লিঃ, ৯/এফ, মতিঝিল, ঢাকা।
১৬. চেয়ারম্যান/ব্যবস্থাপনা পরিচালক, চট্টগ্রাম স্টক এক্সচেঞ্জ লিঃ, ১০৮০, শেখ মুজিব রোড, আগ্রাবাদ, চট্টগ্রাম।
১৭. সভাপতি, মার্চেন্ট ব্যাংকার্স এসোসিয়েশন, ইউসুফ চেম্বার (৭ম ফ্লোর), ২০ দিলকুশা, ঢাকা।
২০. চেয়ারম্যান/প্রেসিডেন্ট, এসেট ম্যানেজমেন্ট কোং এন্ড মিউচ্যুয়াল ফান্ডস।

(মোহাম্মদ সানাউল আলম সমু)
যুগ্মপরিচালক
ফোন- ২৫৫৬৬৫০০১-৬/২০২৮৪

BANGLADESH FINANCIAL INTELLIGENCE UNIT

Guidelines on Electronic Know Your Customer (e-KYC) for Insurance Companies and Capital Market Intermediaries (CMIs)

Preface

Bangladesh is one of the fastest-growing economies in the world and has the potential to become a trillion-dollar economy within the next decade. In this context, strengthening financial inclusion, promoting innovation in financial services, and ensuring the integrity of the financial system remain key national priorities. Sustainable Development Goal (SDG) 1, particularly Target 1.b, emphasizes the establishment of sound policy frameworks based on pro-poor and gender-sensitive development strategies to support accelerated investment in poverty eradication. At the international level, the Financial Action Task Force (FATF) encourages jurisdictions to promote financial inclusion through the application of a risk-based approach.

The implementation of Electronic Know Your Customer (e-KYC) mechanisms can play a significant role in facilitating secure, efficient, and inclusive financial services. e-KYC enables financial institutions to onboard customers remotely and digitally while maintaining compliance with Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) obligations. Furthermore, The Government of Bangladesh identified the promotion of FinTech and RegTech as a strategic priority to strengthen financial inclusion and enhance cyber security through the National Strategy for Prevention of Money Laundering and Combating Financing of Terrorism (2019–2021). In this regard, Strategic Objective 08 of the strategy emphasizes the promotion of technology-driven financial services, while Action Item 9 sets a target to implement e-KYC/Digital KYC across financial institutions. In light of these developments, the Bangladesh Financial Intelligence Unit (BFIU) issued the first e-KYC Guideline on 08 January 2020 for financial institutions.

This document introduces an updated version of the e-KYC Guideline for the insurance companies/CMISs, developed through extensive consultation with key stakeholders and informed by relevant international best practices. The aim of this revised guideline is to facilitate secure digital onboarding, strengthen AML/CFT compliance, and enhance the efficiency and accessibility of financial services.

BFIU expects Insurance Companies/CMIS to implement this updated guideline by 31st December 2026. Effective implementation of e-KYC will help these institutions improve service delivery by reducing operational costs and processing time, while supporting sustainable business growth. At the same time, it will strengthen safeguards to prevent the misuse of financial products, services, and delivery channels for money laundering, terrorist financing, and related predicate offences mentioned in the Money Laundering Prevention Act, 2012 (Amended 2015).

Insurance Companies/CMIs are free to adopt the technology solutions and operational models which is most appropriate to their business environment, including the models suggested in this guideline. However, institutions must ensure full compliance with the procedural and control requirements of the selected model.

Abbreviations

Acronyms	Full Forms
AI	Artificial Intelligence
BB	Bangladesh Bank
BFIU	Bangladesh Financial Intelligence Unit
BTRC	Bangladesh Telecommunication Regulatory Commission
CDD	Customer Due Diligence
CDBL	Central Depository of Bangladesh Limited
CMI	Capital Market Intermediary
DNFBPs	Designated Non-Financial Business and Professions
EDD	Enhanced Due Diligence
e-KYC	Electronic Know Your Customer
FATF	Financial Action Task Force
KYC	Know Your Customer
MFS	Mobile Financial Service
ML/TF	Money Laundering & Terrorism Financing
NRA	National ML/TF Risk and Vulnerability Assessment
NID	National Identification Database
OCR	Optical Characteristic Recognition
SDD	Simplified Due Diligence
SIM	Subscriber Identity Module
SDG	Sustainable Development Goal
PEP	Politically Exposed Persons
2FA	Two Factor Authentication

1. Introduction

1.1 Background

The concept of Know Your Customer (KYC) within the financial sector and Designated Non - Financial Business and Professions (DNFBPs) started only a few decades back. It got momentum when FATF came forward with a set of recommendations for the prevention of money laundering and financing of terrorism. Within the FATF standards, KYC had emerged as one of the main preventive measures or tools to protect financial institutions abusing from criminal activities.

The FATF Recommendation No. 10 requires financial institutions to conduct KYC, and Customer Due Diligence (CDD) either simplified or enhanced based on the customer risk profile as well as ongoing CDD measures. It also requires that CDD should be undertaken by the financial institutions while establishing business relationships with customers.

The CDD measures to be taken by the financial institutions as per the FATF standards are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information.
(b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institutions (e.g. insurance, securities) are satisfied that it knows who is the beneficial owner. For legal persons and arrangements, this should include financial institutions understanding the ownership and control structure of the customer.
(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business, and risk profile, including, where necessary, the source of funds. The Financial institutions should be required to apply each of the CDD measures and should determine the extent of such measures using a risk-based approach (RBA) following the Interpretive Notes to this Recommendation. The relevant identification data may be obtained from a public register, from the customer, or from other reliable and independent sources.

In 2017, the FATF provided a specific supplement to the 2013 Guidance on AML/CFT Measures and financial inclusion, focusing specifically on CDD and financial inclusion. The Guideline highlights risk mitigation measures that Financial Institutions should apply commensurate with the nature and level of risks identified, to mitigate the risks. It also presents different CDD approaches which can be implemented to facilitate financial inclusion and remove obstacles linked to the verification of the customer's identity, either a broad understanding of the reliable and independent source of information or simplified due diligence measures.

FATF standards apply to both traditional and digital financial services. Digital financial services cover financial products and services, including payments, transfers, savings, credit, insurance, and securities. They are delivered via digital/electronic technology such as e-money (initiated either online or on a mobile phone), payment cards, and regular Insurance Companies/CMIs accounts.

In Bangladesh, section 25 of the Money Laundering Prevention Act (MLPA), 2012 (as amended in 2015) requires financial institutions to collect the complete and correct identity of customers while establishing business relationships with their potential customers. Rules 6 to 12 of the Money Laundering Prevention (MLPR) Rules 2019 provide a detailed framework to conduct customer due diligence for financial institutions, where Rule no. 10 provides the legal basis to adopt a risk-based approach in case of customer due diligence, i.e., application of simplified measures for lower risk scenario and vis-à-vis enhanced measures for higher risk scenario. With the spirit of those laws, Bangladesh Financial Intelligence Unit (BFIU) has issued several circulars and circular letters instructing financial institutions to conduct know-your-customer programs, which starts from customer onboarding.

In several countries, the expansion of digital financial services has been supported by the implementation of a tiered KYC approach. However, in Bangladesh for a lower threshold of transactions and limited wallet size and considering the risk, BFIU directed for Simplified Due Diligence (SDD) for mobile financial services, digital financial services, and other low or limited risks insurance, and securities products. The scope of the applicable measures of SDD is limited and it applies only when the products or services are assessed as low risk.

The lower ML/TF risk situations may permit the use of digital ID systems for simplified due diligence, for example, when the ML/TF risks of potential customers are lower, a digital ID system for identity proofing may be appropriate. Conversely, for higher ML/TF risk situations, financial institutions may adopt additional independent means of reliable information to verify customers' identity details. It is also observed in several countries that several low-risk accounts are being created and ultimately controlled by one bad actor. Therefore, additional measures are required to ensure that this type of ML/TF risk is mitigated, for example, by

putting restrictions on the use of the account.

In Bangladesh, the Election Commission of Bangladesh holds the citizens' (18 years and above) identity data with their biometrics (facial image and 10 fingerprint slaps) and it has a higher level of assurance and authenticity, whereby financial institutions can have access to check the authenticity of customer-provided identity data and biometrics by using this database. Therefore, this e-KYC Guideline is based on the national ID card and the bio-metrics data stored against each NID card.

This e-KYC guideline contains a set of instructions for the Insurance Companies/CMIs to enable them to conduct customer due diligence by digital means.

1.2 Scope

This Guideline shall be known as Electronic Know Your Customer (e-KYC) Guidelines which deals with electronic customer onboarding, identification, and verification of customer identity, creation of customer digital KYC profile as well as risk grading of the customer by digital means. The scope of this Guideline will be as follows:

(a) The provisions of this Guideline shall apply to natural persons;

(b) The requirements of this guideline shall be applicable based on the risk exposures of the customers of the financial institutions. For example, for an assessed low-risk customer, the Insurance Companies/CMIs shall be required to conduct simplified e-KYC which includes electronic customer onboarding, verifying customer identity, and preserving customer profile digitally, whereas, the Insurance Companies/CMIs shall be required to conduct regular and enhanced e-KYC which includes electronic customer onboarding, verifying customer identity, digitally preserving KYC and risk grading for a customer with a regular and higher risks scenario;

(c) The e-KYC requirement of this Guideline is based on biometric verification; therefore, a client whose status is a legal person or legal arrangement is excluded from the obligation of this Guideline. In this case, KYC and CDD norms for the legal person or legal arrangement shall be undertaken as per the provisions of the MLPA 2012, Anti-Terrorism Act (ATA), 2009, the MLP Rules, 2019, Anti-Terrorism (AT) Rules 2013; and instructions contained in the circulars and guidelines issued by the BFIU time to time.

(d) Where e-KYC attempts failed due to any technical reason, the traditional KYC approach should be followed for the natural person.

(e) Non-resident Bangladeshis (NRB) may be onboarded through eKYC as long as they have valid NIDs, and the insurance companies/CMIs have the requisite system in place (through their app/web platform).

1.3 Objectives

The key objective of promoting e-KYC is that it can provide ample scope for quick onboarding of customers by verifying customer identity through digital means which can leverage saving of time and provide ease both for the client and service providers. Additionally, e-KYC can save institutional costs as well as foster greater financial inclusion. Therefore, the basic objectives of implementing e-KYC are as follows:

- Enhancing the growth of financial inclusion;
- Protect the financial sector from abuse of criminal activities;
- Ensure integrity and stability of the financial sector;
- Manage ML/TF risks;
- Reduction of costs related to customer onboarding and managing CDD; and
- Promote fintech services

2. E-KYC Process

2.1 Definitions

(a) "e-KYC Process" refers to a combination of paperless customer onboarding, promptly identifying and verifying customer identity, maintaining a KYC profile in a digital form, and determining customer risk grading through digital means.

(b) "Simplified e-KYC" refers to a process where a customer can be onboarded and verify customer identity electronically using a simplified digital KYC form in case of a proven lower-risk scenario. No risk grading will be required while onboarding the customer. However, sanction screening should be undertaken, and a KYC review shall be done in every five years.

(c) "Regular e-KYC" refers to a process where a customer can be onboarded and verify customer identity electronically; a prescribed digital KYC form is required to be filled in and stored as well as a risk grading exercise is required to be documented electronically. However, based on the risk grading exercise where the customer rated as high risk or some specific scenarios, for example for Influential Persons (IPs), some Enhanced Customer Due Diligence (EDD)[1] is required to be undertaken as per provided sample in section 6.2 of this Guideline.

[1] The EDD measures should include collection of additional information, monitoring of account activity and approval from Chief AML/CFT Compliance officer.

(d) “Transaction” means the deposit, withdrawal, exchange, or transfer of funds in any currency, whether conducted in cash, by cheque, payment order, other instruments, or through electronic or other non-physical means;

(e) “Suspicious Transaction” means a transaction as defined in Section 2(z) of the MLPA, 2012.

(f) “Customer” means any person who engages in, or seeks to engage in, a financial transaction or activity with an institution and includes a person on whose behalf such transaction or activity is conducted.

(g) “Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner.

(h) “Face-matching” refers to customer onboarding using a face-matching model where customer face biometrics will be used as a main identifier of a person’s identity along with the national ID number of the election commission of Bangladesh.

(i) “Fingerprint matching” refers to customer onboarding using a fingerprint matching model where the customer fingerprint data stored within the NID will be used as a main identifier of a person’s identity along with the national ID number of the election commission of Bangladesh.

(j) “Periodic Updation” means steps taken to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records.

(k) “Influential Persons” (IPs) are individuals who are or have been entrusted domestically with prominent public functions, for example Head of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

2.2 Process

The traditional KYC process requires the KYC form to be filled out and the photo ID and signature of the customer along with the required documents are collected. All the way it's a manual process. However, e-KYC is a digital process where insurance companies/CMIs can open a customer account by filling up a digital form, taking photographs on the spot, and authenticating the customer’s identification data (ID No., biometric information, address proof) instantaneously. Such biometric information or digital signatures or electronic signatures may be used for transaction authentication as well. The customer onboarding process may undertake via the following means:

(a) **Assisted customer onboarding:** Where an Insurance Companies/CMIs or its nominated agent or third-party visits the customer or the customer visits the Insurance

Companies/CMIs or its nominated agent or third party's premises and opens an account with the direct assistance of the Insurance Companies/CMIs or its nominated agent or the third party; and

(b) **Self check-in:** Where the customers can onboard on their own by using a kiosk, smartphone, or personal computer. Self check-in shall be allowed for the face-matching model only as described in section 3.3 of this Guideline document.

2.3 Applicability

e-KYC shall only be applicable to natural persons who have valid NID. Natural persons without NID and a legal entity or arrangement have to follow the KYC norms as prescribed by the BFIU from time to time. Therefore, 'simplified' and 'regular' e-KYC norms shall be applicable based on the threshold and risk mentioned in this Guideline. As such this Guideline is applicable for the Insurance Companies/CMIs licensed by the Insurance Development and Regulatory Authority/ Bangladesh Securities and Exchange Commission. The threshold mentioned in this Guideline may be changed from time to time by the BFIU. Insurance companies/CMIs shall conduct paper-based customer onboarding and simplified or regular KYC and CDD measures if any customer is unable to onboard with this e-KYC mechanism.

2.3.1. Insurance Companies/CMIs Sector Products Under Simplified e-KYC

The scope of simplified e-KYC covers the following which may be revised by the BFIU based on identified risks and consultation with relevant stakeholders from time to time:

(a) **Securities Market Products (This includes customer initial deposit plus amount transferred through link account) :** Deposit to the BO account up to BDT 1,500,000;

(b) **Insurance Products:**

Life Insurance: The sum assured up to BDT 2,000,000 with an annual premium not exceeding BDT 250,000.

Non-Life Insurance: Any sum premium not exceeding BDT 250,000.

2.3.2 Financial Sector Products Under Regular e-KYC

Insurance Companies/CMIs Products

Other Insurance Companies/CMIs products except the products mentioned in section 2.3.1;

3. Customer Onboarding-Simplified

3.1 Customer Onboarding Models

Insurance companies/CMIs are allowed to follow customer boarding under this Guideline, which is based on the national identification documents, information stored within a specific NID plus any one of the bio-metric verification out of fingerprint matching and face matching[2]. The customer onboarding should also be covered self check-in, check-in with the assistance of service providers, and other relevant means as required necessary. If in any phase of the mentioned process, the customer fails to onboard due to a technical error, the traditional paper KYC process should be offered to the customer.

Electronic customer onboarding involves multiple activities. An efficient customer onboarding starts from clients' identity information and can be segmented into the following steps:

a) Data capture and generation;

b) Identity verification;

c) Sanction and other screening;

d) Account opening;

e) Customer profiling (e-KYC Profile); and

f) Customer risk grading (as applicable).

To undertake e-KYC, this guideline suggests initially following two biometric-based models of customer onboarding which are as follows:

(a) Customer onboarding by using fingerprint; and
(b) Customer onboarding by matching faces.

Moreover, insurance companies/CMIs can also introduce other innovative models using biometric beyond these two models having prior approval from concerned regulatory authority and BFIU.

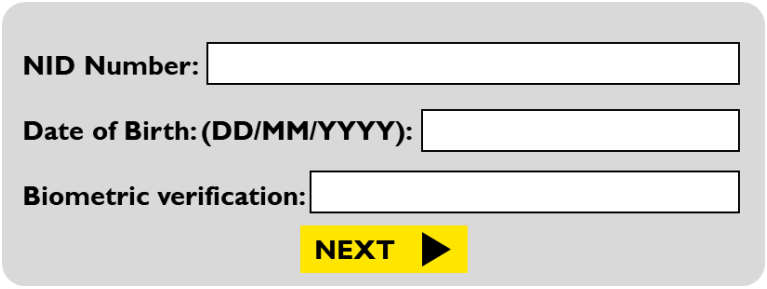
3.2 Customer Onboarding by Using Fingerprint

Customer onboarding by using fingerprint matching is one of the commonly used methods where customer fingerprints will be used as the main identifier of a person's identity. The

[2] Insurance companies/CMIS are free to choose any model based on their preparation and infrastructure.

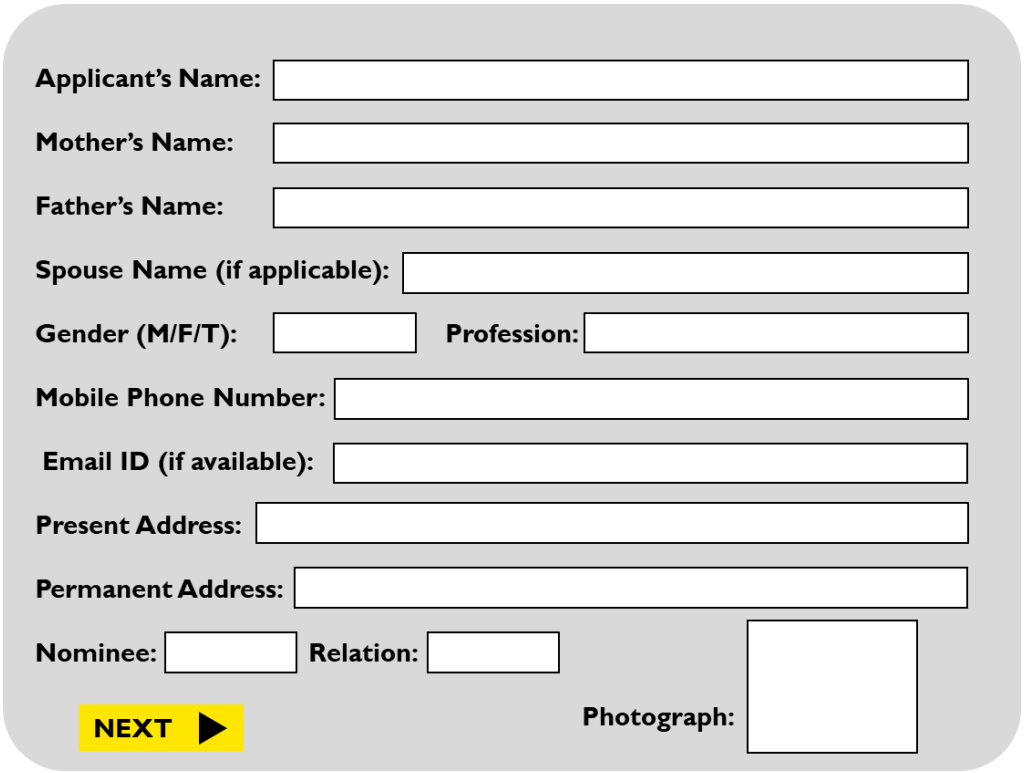
minimum generic approach for this model will be as follows:

a. First Step



In this step, a customer approaches a Insurance Companies/CMIs or its agent or a Insurance Companies/CMIs or its agent approaches a customer for BO account opening or policy opening process using e-KYC. Then, the customer will provide his or her NID. The Insurance Companies/CMIs or its agent inserts NID the number and Date of Birth (DOB) into the specified template, and collects the fingerprint of the customer, then presses the Next button. The Election Commission database holds data for all 10 fingers, but for e-KYC purposes matching one finger should suffice (the customer may use any preferred finger). A maximum of 10 (ten) fingerprint attempts is allowed per session. Two sessions are the maximum limit for a day. If the fingerprint matching fails in the sessions, the customer can re-try after 24 hours. If fingerprint verification fails in 03 (three) sessions, the insurance Companies/CMIs must offer the customer face recognition. In the case of failed matching attempts, the insurance/security companies should keep a record of such instances as failed e-KYC. Once the Insurance Companies/CMIs or its agent presses the Next button the information of NID number, DOB, and fingerprint data will be matched with the NID database, if the data is matched, then the next template will appear.

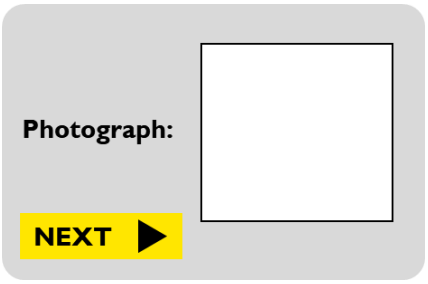
b. Second Step[3]



In step two, all necessary information will be fetched up in the above digital format and additional input may be punched to fulfill the whole template. Optical character recognition (OCR) should be used to capture the NID data. The NID data should be captured in both Bangla and English. The nominee's name, relation to the customer, and photo can be manually entered by the respective agent, but the customer's personal information should be captured from the OCR. The phone number or email ID (customer preference) should be mandatory for account opening notifications. Alternatively, the respective agent may input the information manually after consulting the customer. On completion of personal information, the Insurance Companies/CMIs or agent will press the Next option.

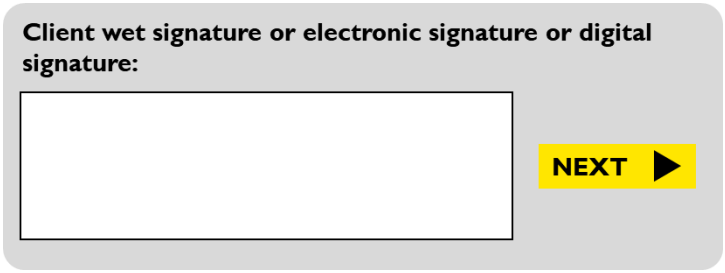
[3] The template given here is for the minimum required information. The financial institutions may add a few more fields where necessary, financial institutions may add additional fields for the additional nominee(s) and/ or where additional guardian information is required for the minor account.

c. Third Step



In step three, the Insurance Companies/CMIs or its agent or client will capture or upload the customer's photograph, then press the Next option.

d. Fourth Step[4]

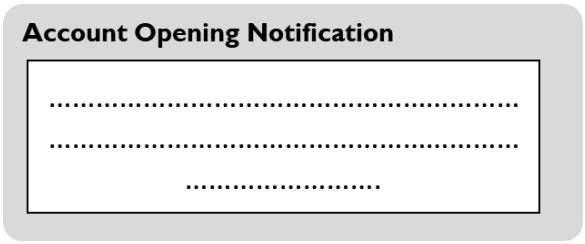


In step four, the customer's wet signature (signature using a pen), an electronic signature (signature using devices), or a digital signature, or image of signature is required to be preserved for future reference. A digital signature or a PIN may be generated and used if the customer is unable to provide a wet signature. Using a digital signature or PIN will only be applicable for low-risk accounts and signatures must be provided for high-risk accounts.

e. Fifth Step

In step five, after the completion of all the processes, the system will generate a notification of an account opening in the process. After completion of the necessary sanction and other screening, an account opening confirmation notification should be sent to the customer.

[4] Where necessary, the financial institutions may collect physical signatures at a later stage and preserve them digitally for further future use.



The simplified customer onboarding process will be completed once the client gets a notification from insurance companies/CMIs. The notification should contain the account name and number, the customer's branch, account type, and the service number of the customer. The notification should be sent via registered mobile number (SIM) and email ID (if available). In case of a failed e-KYC, a failure notification is to be sent. However, at any point in the relationship, the Insurance Companies/CMIs may ask for additional information from the customer and will preserve it in the digital KYC profile of the customer. If the client does not receive any notification due to technical reasons, he/she should call the help desk of the Insurance Companies/CMIs to report the problem. A customer care number should be provided by insurance companies/CMIs on their website/app.

In the case of joint customer (more than one) onboarding, a similar process should be followed. All the fields mentioned in step two are the minimum requirements, however, Insurance Companies/CMIs may add a few fields where necessary.

In case there are 3 failed fingerprint identification tries in a single session, insurance companies/CMIs should attempt face matching.

3.2.1 Required Technology

The electronic customer onboarding and the e-KYC process require a technology platform. Therefore, based on the simplified e-KYC model at a minimum, the following technology and instruments may be used to complete the process;

a. Software/App/Program compatible with the above process;
b. Internet connection;
c. Online connection to the NID verification server[5];
d. Fingerprint capturing devices;
e. Electronic signature capturing devices (where necessary) etc.

[5] Refers to the NID database either held by the NID Wing of the Election Commission and/or any other Government-vetted Authority for identity verification.

3.2.2 Sanction and Other Screening

The full-fledged account procedures will be completed by completion of sanction and other necessary screening which includes as follows:

a. UNSCRs screening;
b. Adverse media screening (where necessary); and
c. Internal or external exit list (where necessary).

3.2.3 Audit Trail of Customer's KYC Process

To maintain an audit trail, an Insurance Companies/CMIs or their nominated third parties are required to preserve a digital KYC profile and relevant logbook, even for low-risk or financial inclusion products, which should include the following:

a. Customer details (name, contact, address) with photograph;
b. Customer NID image (both sides);
c. Customer signature (where necessary); and
d. Customer risk review process (once in 5 years);

The Insurance Companies/CMIs should maintain a digital log for all successful and unsuccessful client onboarding, matching parameters, etc. for further work and audit trail. All the data should be preserved and stored digitally for further internal and external audit purposes. The sample e-KYC profile, at a minimum, should look as per 6.1.

3.2.4 Matching parameters[6]

As the electronic onboarding requires matching the customer's ID stored data with the national identification database, the following elements or information are required to be matched as per described percentage:

Particulars	Parameter
Applicant's Name	Yes
Date of Birth	Yes
Fingerprint	Yes
NID number	Yes
Fathers' Name (If Available)	Yes
Mothers' Name (If Available)	Yes
Spouses' Name (If Available)	Yes

[6] Applicant's name and parents' name field may be left as an editable form for correction of spelling mistakes, however, date of birth and NID number should be kept in un-editable form.

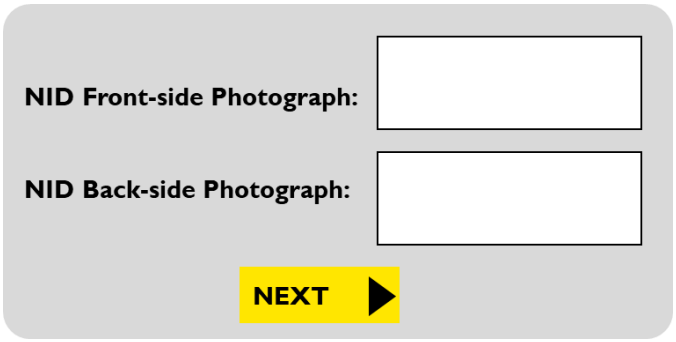
3.2.5. Security Measures

The Insurance Companies/CMIs may use additional security measures in the customer onboarding process which may include checking the phone number by generating One-time PIN codes and other measures as deemed necessary. Additionally, the security of data recorded and preserved under this e-KYC should be maintained properly by the Insurance Companies/CMIs so that no customer data can be hacked or compromised. This Guideline also suggests preserving customer data on locally hosted servers or private cloud servers and putting in place necessary data protection and data security measures as prescribed by the government of Bangladesh.

3.3 Customer Onboarding by Using Face-Matching

The Insurance Companies/CMIs may adopt customer onboarding using a face-matching model where customer face biometrics will be used as a main identifier of a person's identity along with the national ID number and date of birth. The following steps will be required for the onboarding of a customer by using face matching model:

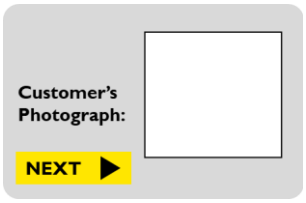
a. First Step[7]



In this step, a customer approaches a Insurance Companies/CMIs or its agent or a Insurance Companies/CMIs or its agent approaches a customer or customer engaged in self check-in for account opening process by using e-KYC procedures. Then, it is required to first capture the photo or scan the front side of the customer's NID, followed by the back page. Optical character recognition (OCR) should be used to capture the NID data both in Bangla and English. In the backend, all NID data will be stored in the appropriate fields within a textual format.

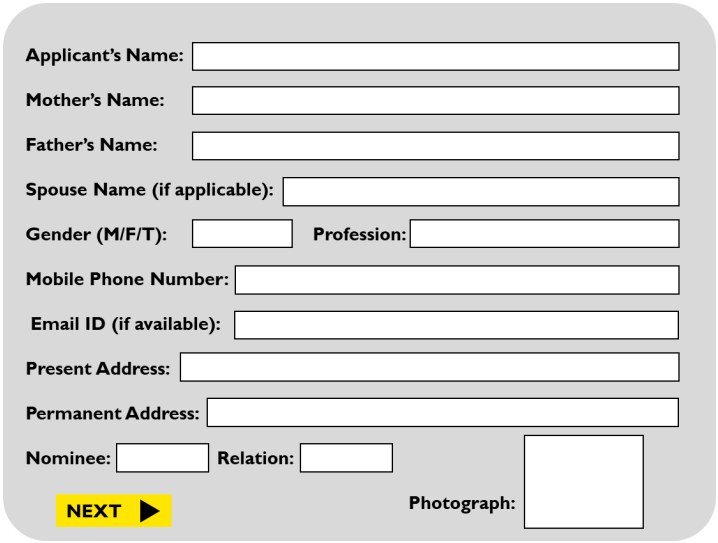
[7] The system should be capable enough to capture front page of NID first, followed by back page.

b. Second Step[8]



In step two, the Insurance Companies/CMIs or its agent or customer will take an appropriate photograph of the customer's face by using a high-resolution camera or webcam. While taking the picture, the agent or the client is required to be tactful enough to take the face only of the customer as well as ensure the visible quality of the photograph. After capturing the photo of the customer, it will be matched with the customer's photo stored in the EC server. A maximum of 10 (ten) tries are permitted in a single session. Two sessions are the maximum limit for a day within 24 hours. The insurance companies/CMIs shall allow maximum 03 (three) sessions for a customer onboarding. Alternatively, if the face does not match for any customer, then fingerprint verification or paper KYC options are to be offered to onboard a customer. In the case of self check-in, the customer is required to capture a live selfie with proper light and camera frame[9]. In the case of failed matching attempts, the Insurance companies/CMIs should keep a record of such instances as failed e-KYC.
For further clarification regarding photo capture, refer to Annexure-2.

c. Third Step[10]



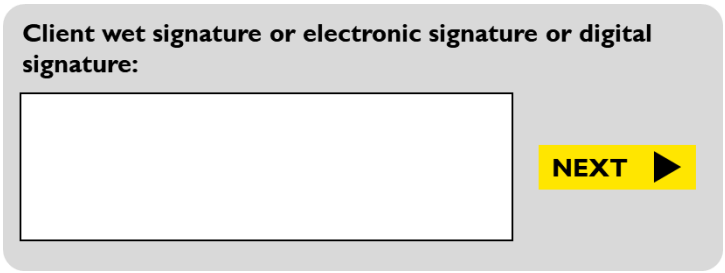
[8] There should a mechanism that system only captured real persons' picture only.

[9] There should be a mechanism that the system only captures real persons' pictures only.

[10] This template given here is the minimum information. The financial institutions may add a few more fields where necessary. Where necessary, reporting entities may add additional fields for the additional nominee(s) and/ or where additional guardian information is required for the minor account.

In step three, all necessary information will be fetched up from the NID through OCR in the above digital format. Additional input such as the nominee's name, relation to the customer, and the nominee's photo should be inserted by insurance companies/CMIs to fulfill the whole template. Alternatively, the Insurance companies/CMIs agent may input all of the information manually after consulting the customer. The phone number or email ID (customer preference) should be mandatory for account opening notifications.

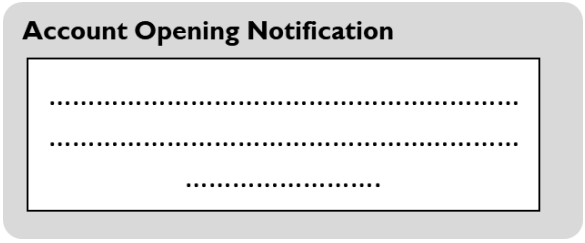
d. Fourth Step[11]



In step four, the customer's wet signature (signature using a pen), an electronic signature (signature using devices), or a digital signature is required to be preserved for future reference. A digital signature or a PIN may be generated and used if the customer is unable to provide a wet signature. Using a digital signature or PIN will only be applicable for low-risk accounts and wet/electronic signatures must be provided for high-risk accounts.

e. Fifth Step

In step five, after the completion of all the processes, the system will generate a notification of an account opening in the process. After completion of the necessary sanction and other



screening, an account opening confirmation notification should be sent to the customer.

[11] Where necessary, the reporting entity may collect a physical signature at a later stage and preserve it digitally for further future use.

The simplified customer onboarding process will be completed once the client gets a notification from the financial institution. The notification should contain the account name and number, the customer's branch, account type, and the service number of the customer. The notification should be sent via registered mobile number (SIM) and email ID (if available). In case of a failed e-KYC, a failure notification is to be sent. However, at any point in the relationship, the Insurance Companies/CMIs may ask for additional information from the customer and will preserve it in the digital KYC profile of the customer. If the client does not receive any notification due to technical reasons, he/she should call the help desk of the Insurance Companies/CMIs to report the problem. A customer care number should be provided by Insurance companies/CMIs on their website/app.

In the case of joint customer (more than one) onboarding, a similar process should be followed. All the fields mentioned in steps two and three are the minimum requirement, however, financial institutions especially Insurance Companies/CMIs may add a few fields where necessary.

3.3.1 Required Technology

At a minimum, the customer onboarding via the face-matching model requires the usage of the following technology to complete the whole customer onboarding process;

a. Software/App/Program compatible with the above process;

b. Internet connection;

c. Smartphone or desktop computer with a high-resolution webcam;

d. Online connection to the NID verification server[12];

e. Electronic signature capturing devices (where necessary) etc.

3.3.2 Sanctions and Other Screening

The full-fledged account procedures will be completed by completion of sanction and other necessary screening which includes as follows:

f. UNSCRs screening;

g. Adverse media screening (where necessary); and

h. Internal or external exit list (where necessary).

[12] Refers to the NID database either held by the NID Wing of the Election Commission and/or any other Government-vetted Authority for identity verification.

3.3.3 Audit Trail of Customer Profile

To maintain an audit trail a Insurance Companies/CMIs or their nominated third parties are required to preserve a digital KYC profile and relevant logbook, even for low-risk or financial inclusion products, which should include the followings:

a. Customer details (name, contact, address) with photograph;

b. Customer ID image (both sides);

c. Customer signature (where necessary); and

d. Customer risk review process (once in 5 years);

The Insurance Companies/CMIs should maintain a digital log for all successful and unsuccessful clients onboarding, matching parameters, etc. for further use and audit trail. All the technical data should be preserved and stored digitally for further internal and external audit purposes. The sample e- KYC profile, at a minimum, should look as per section 6.1.

3.3.4 Matching parameters[13]

As the electronic onboarding requires matching the customer's ID stored data with the national identification database, the following elements or information are required to be matched as per described percentile:

Particulars	Parameter
Applicant's Name	Yes
Date of Birth	Yes
Face	Yes
NID number	Yes
Fathers' Name (If Available)	Yes
Mothers' Name (If Available)	Yes
Spouses' Name (If Available)	Yes

3.3.5 Security measures

The Insurance Companies/CMIs may use additional security measures in the customer onboarding process which may contain checking the phone number by generating PIN codes and other measures as deemed necessary. Additionally, the security of the data recorded and preserved under this e-KYC should be maintained properly by the Insurance Companies/CMIs

[13] Applicant's name and parent's name fields may be left as editable form, however, date of birth, and NID number should be kept in un-editable form.

so that no customer data can be hacked or compromised. This Guideline also suggests preserving customer data in a locally hosted server or a private cloud server and putting in place necessary data protection and data security measures as prescribed by the government of Bangladesh.

4. Customer onboarding- Regular measure

Insurance companies/CMIs are encouraged to use electronic onboarding and e- KYC procedures for the products and services which do not fall under proven low-risk or limited risks as well. This means electronic onboarding and e- KYC procedures are also applicable for any sort of financial product.

Both the technology-based models i.e., fingerprints and face-matching technologies are applicable for regular onboarding and managing KYC. Similarly, such an onboarding process is only applicable to a natural person who has a valid NID.

Initially, the onboarding process for the regular e-KYC is similar, however, it requires few modes of additional information and conducts additional customer due diligence compared to the simplified method. The reporting entities are required to create digital customer KYC profiles and risk grading exercises digitally during the regular e-KYC. This means similar step-by-step[14] procedures have to be followed in the case of different models (fingerprint and face matching) as discussed above to complete the regular e-KYC procedures.

Therefore, regular e-KYC includes the following elements:

a. A digital template with more information compared to simplified e-KYC;

b. A more stringent KYC profile of the customer;

c. Screening of customers other than UN Sanctions (for example PEPs/IPs, Beneficial Owner, Adverse Media, Internal External list checking, etc.); and

d. Risk grading exercise.

[14] All steps mentioned in this Guideline are generic; the financial institution may reorganize this step-by-step process where necessary.

Along with the process of digital onboarding already discussed above, the digital information template at a minimum required for regular e-KYC would be as follows:

Applicant's Name:

Mother's Name:

Father's Name:

Spouse Name:

Gender (M/F/T): **Date of Birth:**

Profession: **Monthly income:** **Sources of Fund:**

Mobile Phone Number:

Present Address: **Nationality:**

Permanent Address:

Nominee : **Date of Birth:** **Relation:**

Photograph:

NB:

i. **If the applicant is minor then they should proceed with traditional methods of account opening;**
ii. **Incorporate 'add' the following field if the nominee is 'Minor'**
iii. **Name of minor nominee**
iv. **Name of Guardian**
v. **Address**
vi. **Relation**
vii. **NID of Guardian**
viii. **Photograph of Guardian**

The customer onboarding process and instructions as discussed above for the simplified measures will be similar to regular e-KYC. After opening an account Insurance Companies/CMIs may collect additional information and a customer wet signature to create a full digital profile of the client.

4.1 Required Technology

The same technologies that are mentioned in this Guideline for simplified e-KYC (section 3.2.1 and section 3.3.1) also apply to regular e-KYC.

4.2 Sanctions and other screening

The screening mechanism for regular e-KYC is quite stringent compared to the simplified one. The full-fledged account procedures will be completed by completion of sanctions and other necessary screening which includes as follows:

a. UNSCRs screening;

b. IPs Screening;

c. Identification of beneficial ownership (if any);

d. Adverse media screening;

e. Risk grading of the customer;

f. Customer Due Diligence template;

g. Enhanced Due Diligence (if needed).

4.3 Audit trail of customer profile

To maintain an audit trail a Insurance Companies/CMIs or their nominated third parties are required to preserve a digital KYC profile and relevant log book or data which should include the followings:

a. Customer details (Name, contact, address) with photograph;

b. Customer ID image (both sides);

c. Customer signature (where necessary);

d. Risk grading of the customer (where necessary);

e. Customer Due Diligence template (where necessary)

The Insurance Companies/CMIs should maintain a digital log for all successful and unsuccessful e-KYC onboarding processes for further work and audit trail. All the technical data should be preserved and stored digitally for further audit purposes. The sample e-KYC profile, at a minimum, should look as per 6.2.

For customers that have moved up the risk-grading from low-risk to high-risk, Insurance companies/CMIs should wait one month till the customer responds to EDD calls before temporarily closing the account. However, if any irregular activity is detected from the account, closure may happen sooner.

4.4 Matching parameters

The matching parameters mentioned in the simplified e-KYC will apply to regular e-KYC.

4.5 Security measures

The Insurance Companies/CMIs may use additional security measures in the customer onboarding process which may contain checking the phone number by generating pin codes and other measures as deemed necessary. Additionally, the security of the data recorded and preserved under this e-KYC should be maintained properly by the Insurance Companies/CMIs so that no customer data is hacked or compromised. This Guideline also suggests preserving customer data in a locally hosted server or cloud server and putting in place necessary data protection and data security measures as prescribed by the government of Bangladesh.

To ensure better protection of the stored data, the following instructions should be followed:

i. The e-KYC system should use HTTPS for communication.
ii. "HTTP" should not be allowed and should be forced to redirect to HTTPS.
iii. The e-KYC system application and external APIs should only be accessible via authorization using standard authorization methods such as login credentials, bearer token, and jwt token.

5. Other Relevant Issues

5.1 Record Keeping

The Insurance Companies/CMIs should maintain all sorts of digital KYC data and log until five years after the closure of the account or business relationship. The digital data shall contain customer onboarding, customer identity verification, KYC profile, risk grading exercise; transaction-related data and their analysis; all sorts of correspondence with the customer; data collected later for CDD purposes; and all other relevant files.

The authorized maker (customer in case of self-check-in, and the FI agent conducting e-KYC) and checker in the e-KYC system can access e-KYC data stored in a financial institution. For system management purposes, the system administration team and the system auditor can access the stored e-KYC data through an authorized channel.

Digital footprint and the log should contain but not be limited to information collected during clients' identity verifications and other relevant information related to the screening measures is also required to be preserved. The financial institutions also may collect other complementary data (such as geo-location, IP addresses, etc.) which could also support ongoing due diligence.

5.2 Reliance on Third Parties

To implement the e-KYC, the Insurance Companies/CMIs may rely on third-party technology providers either fully or partially to implement e-KYC. Though a Insurance Companies/CMIs may be engaged with a third party, the ultimate responsibility still lies with them. This means financial institutions may rely on another entity or technology provider that satisfies the criteria described above to conduct customer due diligence which covers:

a. Customer identification and verification data from independent and reliable sources;
b. Identify and understand who the beneficial owner(s) is, and
c. Identify the purpose and intended nature of the business and relevant CDD measures digitally.

Yet, the Insurance Companies/CMIs itself should ensure the reliability and authenticity of the data collected. The following condition may apply while engaging with any third party for the Financial Institutions:

- Immediately obtain the necessary information concerning the identity of the customer as mentioned in (a) –(c) above.
- Take adequate steps to satisfy itself that the third party will make available copies of identity evidence or other appropriate forms of access to the data or digital log as mentioned (a) –(c) in the above and this Guideline without delay.
- The activities of the third party shall be regulated under this e-KYC Guidance and will be monitored by the financial institutions.
- The third party shall ensure customer and financial institutions' data protection according to the IT security policy of the Bangladesh Government and the respective prudential and self-regulators.
- Both the third party and the Insurance Companies/CMIs covered under this guidance shall ensure the customer data collected under this guidance shall not be digitally transmitted or transferred outside Bangladesh without prior approval of the prudential regulators and/or BFIU. In this case, BFIU Circular No. 23 dated 31/01/2019 will be applicable.

5.3 Risk Assessment

The Insurance Companies/CMIs shall have to conduct a risk assessment of the new technology-based electronic KYC mechanism to understand how it may be abused and put in place appropriate measures to prevent such abuse as per the circulars and Guidance issued by

BFIU. The Insurance Companies/CMIs is also required to conduct a customer risk assessment as mentioned in 6.3 of this Guideline.

5.4 Implementation

The Insurance Companies/CMIs should implement this regulation by 31st December 2026.

5.5 Transformation of Existing Clients CDD

The Insurance Companies/CMIs may transform their existing clients' CDD-related documents into digital form following the above-mentioned procedures where applicable.

5.6 Transformation from Simplified e-KYC to Regular e-KYC

In cases where a customer intends to upgrade an account opened through simplified e-KYC procedures to a regular e-KYC account, the respective Insurance Companies/Capital Market Intermediary shall obtain the necessary additional customer information and documentation in accordance with section 4 of this guideline. Upon satisfactory verification of the additional information and completion of the required due diligence procedures, the entity shall upgrade the customer's account status from simplified e-KYC to regular e-KYC, ensuring that the account is thereafter subject to the standard monitoring and compliance requirements applicable to regular accounts.

5.7 Periodic Updation of e-KYC

Financial Institutions are to adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once every year for high-risk customers, every two years for medium-risk customers, and once every five years for low-risk customers from the date of opening of the account / last KYC updation. Policy in this regard shall be documented as part of the Insurance company/CMIs's internal KYC policy duly approved by the relevant authority.

No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through the customer's email-id registered with the customer's mobile number registered with the Insurance Companies/CMIs, letter, etc. The declaration form should collect the personal details of the customer, i.e. their name, NID number, and contact number.

Address change: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through the customer's email-id registered with the customer's mobile number registered with the Insurance

Companies/CMIs, and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. The declaration form should collect the personal details of the customer, i.e. their name, NID number, and contact number. Address verification may be done by providing the last utility bill at the customer's new address (as is standard practice).

Accounts of customers, who were minor at the time of opening the account, on their becoming major: In the case of customers for whom the account was opened when they were minor, fresh photographs shall be obtained on their becoming a major, and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Insurance companies/CMIs. Wherever required, insurance companies/CMIs may carry out fresh KYC of such customers.

For customers whose risk grading goes up

due to a change in income source: If the income source of a customer changes and increases in risk grading, and the resultant increase changes the status of the customer from low-risk to high-risk, then it is recommended to undertake Enhanced Due Diligence.

6. e-KYC Profile - Simplified and Regular

6.1 Sample Output of The Simplified e-KYC[15]

Photo Customer		Photo Other	
Applicant's Name:			
Mother's Name:			
Father's Name:			
Spouse Name:			
Date of Birth:		**Gender (M/F/T):**	
Profession:			
Mobile Phone Number:		**Present Address:**	
Permanent Address:			
Nominee:		**Relation:**	
Photograph:		**Specimen:**	

signature/digital signature (where necessary)

Front side of NID	Back side of NID

1. Has UNSCRs check been done? (Yes) (No)
2. Has a review of the customer profile been done (existing customer)? if so, date of review
3. What is the average range of customer transactions (over 6/12 months)?
4. Any other relevant field may be added here

[15] 'Photo Others' shall include the photograph of nominee(s), beneficial owner(s), joint account holder(s), minor(s) or their guardian(s) as applicable.

6.2 Sample Output of Regular e-KYC

Photo Customer	Photo Other

Applicant's Name:

Account number: **Unique account number:**

Mother's Name:

Father's Name:

Spouse Name:

Date of Birth: **Gender (M/F/T):**

Profession: **Monthly income:** **Sources of Fund:**

Mobile Phone Number: **Nationality:** **Present Address:**

Permanent Address:

TIN (if any):

Nominee: **Relation:** **Photograph:**

Front side of NID	Back side of NID

Specimen signature

5. **Has the UNSCRs check been done? (Yes) (No)**
6. **Has risk grading been done? If the assessed risk is high then conduct EDD as per the BFIU circular.**

Risk Type	Overall Score
Regular (< 15)	
High (≥15)	

7. **Is the customer IPs/PEPs? If the client is PEPs or IPs with higher risk, then conduct EDD as per the BFIU circular.**
8. **Is there any adverse media news against the customer? If any then conduct EDD.**
9. **Has the source of und verified/justified? (Yes) (No)**
10. **Has the beneficial ownership been checked? If there is any beneficial owner found, then conduct CDD on the beneficial owner. If the beneficial owner is PEPs, then conduct EDD.**
11. **Are any other documents obtained ?**
12. **Nominee details**
13. **Has the review of the customer profile been done (existing customer)? if so, date of review**
14. **What are the average range and usual patterns of customer transactions (over 6/12 months)?**
15. **Any other relevant field may be added here**

6.3 Form for Customer Risk Grading

6.3.1 Form for Customer Risk Grading for Insurance Companies

1. Type of On-boarding	*Score*
Employee Benefit / Group Channel	*2*
Push-sales through agent	*2*
Agency / Bank	*2*
Walk-in	*3*
Digital and Direct	*2*
2. Geographic Risks:	*Score*
Client is--	
Resident Bangladeshi	*1*
Non-resident Bangladeshi	*3*
3. Type of Customer:	*Score*
Is the client a IP, as per BFIU Circular?	
No	*0*
Yes	*5*
Is the client's family/close associates related to PEP/Chief or High Official of International Organization?	
No	*0*
Yes	*5*
Is the client an IP? or is his family/close associates related to IP?	
No	*1*
Yes (based on assessed risk)	*5*

4. Product Risk (Life Insurance)	*Score*
Ordinary Life	*1*
Universal Life	*2*
Term policy / Accidental & Health (A&H) / Rider / Group Life / Group Medical / Credit Life	*3*
5. Business and Activity Risk	*Score*
(a) Business	
Please pick the applicable option from Annexure-1 and put the relevant score in the next column	……
(b) Profession	
Please pick the applicable option from Annexure-1 and put the relevant score in the next column	
	……
6. Transactional Risks:	*Score*
How much is the client's Average Yearly Transactions Worth?	
<BDT 1 million	*1*
From BDT 1 million to 5 million	*2*
From BDT 5 million to 50 million (5 crores)	*3*
More than BDT 50 million (5 crores)	*5*
7. Transparency Risk	*Score*
The client has provided a credible source of funds	
No	*5*
Yes	*1*

In the case of the Insurance companies, there can be following onboarding channels:

1. Agency Channel; (Selling to individuals through agents)
2. Bank Channel; (Selling to individuals through banks)
3. Employee Benefit / Group Channel; (Selling to corporates through an agent and / or company)
4. Digital and Direct; (Selling Online directly to individual customers)

6.3.2 Form for Customer Risk Grading for Capital Market Intermediaries

1. Type of On-boarding	*Score*
Branch/Relationship Manager	*2*
Direct Sales Agent	*2*
Walk-in	*3*
Internet/Self check-in/Other non-Face to Face	*2*
2. Geographic Risks:	*Score*
Client is--	
Resident Bangladeshi	*1*
Non-resident Bangladeshi	*3*
3. Type of Customer:	*Score*
Is the client a PEP/Chief or High Official of an International Organization, as per BFIU Circular?	
No	*0*
Yes	*5*
Is the client's family/close associates related to IPs/Chief or High Official of International Organization?	
No	*0*
Yes	*5*
Is the client an IP? or is his family/close associates related to IP?	
No	*1*
Yes (based on assessed risk)	*5*

4. Product and Channel Risk:	*Score*
Type of Product	
Individual BO account	*2*
5. Business and Activity Risk	*Score*
(a) Business	
Please pick the applicable option from Annexure-1 and put the relevant score in the next column	……
(b) Profession	
Please pick the applicable option from Annexure-1 and put the relevant score in the next column	
	……
6. Transactional Risks:	*Score*
How much is the client's Average Yearly Transactions Worth?	
<BDT 1 million	*1*
From BDT 1 million to 5 million	*2*
From BDT 5 million to 50 million (5 crores)	*3*
More than BDT 50 million (5 crores)	*5*
7. Transparency Risk	*Score*
The client has provided a credible source of funds	
No	*5*
Yes	*1*

Annexure-1: **Assessing Business and Activity Risk (for 6.3.1 and 6.3.2 item no.5)**

Client Business	*Score*	*Client Profession*	*Score*
Jeweler/Gold/Valuable Metals Business	*5*	*Pilot/Flight Attendant*	*5*
Money Changer/Courier Service/Mobile Banking Agent	*5*	*Trustee*	*5*
Real Estate Developer/Agent	*5*	*Professional (Journalist, Lawyer, Doctor, Engineer, Chartered Accountant, etc.)*	*4*
Promoter/Contractor: Construction Projects	*5*	*Director (Private/Public Limited Company)*	*4*
Art and Antiquities Dealer	*5*	*High Official of a Multinational Company (MNC)*	*4*
Restaurant/Bar/Night Club/Parlor/Hotel	*5*	*Homemaker*	*4*
Export/Import	*5*	*Information Technology (IT) sector employee*	*4*
Manpower export	*5*	*Athlete/Media Celebrity/Producer/Director*	*4*
Firearms	*5*	*Freelance Software Developer*	*4*
RMG/Garments Accessories/Buying House	*5*	*Government service*	*3*
Share/Stocks Investor	*5*	*Landlord/Homeowner*	*3*
Software/Information and Technology Business	*5*	*Private Service: Managerial*	*3*
Travel Agent	*4*	*Teacher (Public/Private/Autonomous Educational Institution)*	*2*
Merchants with over 10 million takas invested in the business	*4*	*Private Sector Employee*	*2*
Freight/Shipping/Cargo Agent	*4*	*Self-employed Professional*	*2*
Automobiles business (New or Reconditioned)	*4*	*Student*	*2*
Leather/Leather Goods Business	*4*	*Retiree*	*1*
Construction Materials Trader	*4*	*Farmer/Insurance companies/CMIs herman/Laborer*	*1*
Business Agent	*3*	*Others: (**Please State Below and circle numerical score as needed**)*	*1..2..3..4..5*
Thread/"Jhut" Merchant	*3*		
Transport Operator	*3*		
Tobacco and Cigarettes Business	*3*		
Amusement Park/Entertainment Provider	*3*		
Motor Parts Trader/Workshop	*3*		
Small Business (Investment below BDT 5 million)	*2*		
Computer/Mobile Phone Dealer	*2*		
Manufacturer (except, weapons)	*2*		
*Others: (**Please State Below and circle numerical score as needed**)*	*1..2..3..4..5*		

Annexure-2: Instructions for photo capture for face-matching

For both assisted and self check-in methods, the live photograph of the customer and their original documents shall be captured in proper light so that they are readable and identifiable. A few pointers to be ensured during the photo capture:

(a) **Use a high-resolution camera:** A high-resolution camera, such as a smart phone camera or webcam, should be used to capture the highest-quality picture possible. This ensures that the details on the photo are clear and visible, making it easier to verify the customer's identity.

(b) **Adequate white lighting:** The room where the photos are taken should have adequate white lighting to ensure that the photo is well-lit, and the details are visible. This is particularly important if the customer is using a webcam in a dimly lit room.

(c) **Capture photos against a white background:** It is preferable to capture the photos against a white background. This helps to remove distractions in the background, making it easier to focus on the customer's face.

(d) **Avoid reflection of light:** During the capturing of the NID front and back photo, it must be ensured that there is no reflection of light which may hinder visibility. Reflections can distort the image, making it difficult to verify the customer's identity.

(e) **Full front side of the face should be visible:** The full front side of the face should be visible during photo capture. This means the customer should be at a forward-facing angle so that the facial features are captured properly. This ensures that the photo is clear and easily recognizable, helping to verify the customer's identity.

(f) **Educate customers about the photo-capturing process:** Insurance companies/CMIs should educate customers about the photo-capturing process to avoid errors during the self-check-in method. This can help customers understand the importance of clear photos and ensure that the photos they submit are of high quality, making it easier to verify their identity.

(g) **Depth Sensing while photo capturing:** Insurance companies/CMIs should ensure the captured photo is of a 3D human body, through depth sensing.

(h) Step-by-step instructions for photo capturing are given below:

i. Find a well-lit area: Look for an area that is well-lit with white lighting. Avoid dimly lit areas or areas with colored lighting, as this can affect the quality of the photo.

ii. Find a white background: Look for a white background to stand against. This could be a white wall or a white sheet. Avoid busy or cluttered backgrounds, as this can be distracting and affect the quality of the photo.

iii. Position yourself correctly: Stand facing forward, with your face fully visible in the camera frame. Make sure that your face is not obscured by hair, clothing, or accessories. Keep your head straight and do not tilt it in any direction.

iv. Hold the camera at eye level: Hold the camera at eye level and make sure it is focused on your face. Avoid holding the camera too high or too low, as this can distort the image and affect the quality of the photo.

v. Take the photo: Once you are in the correct position and the camera is focused on your face, take the photo. Make sure that there are no reflections or glare on the photo, as this can affect its quality.