2-6

# KYC Procedures for Merchant-Onboarding

**Version: 1.6**

**Date: 25/9/2025**

## Approved by

**Sabah K. Al-Ghunaim**

**Chairman**

شركة شبكة الخدمات الآلية
Automated Services Network Co.

## Contents

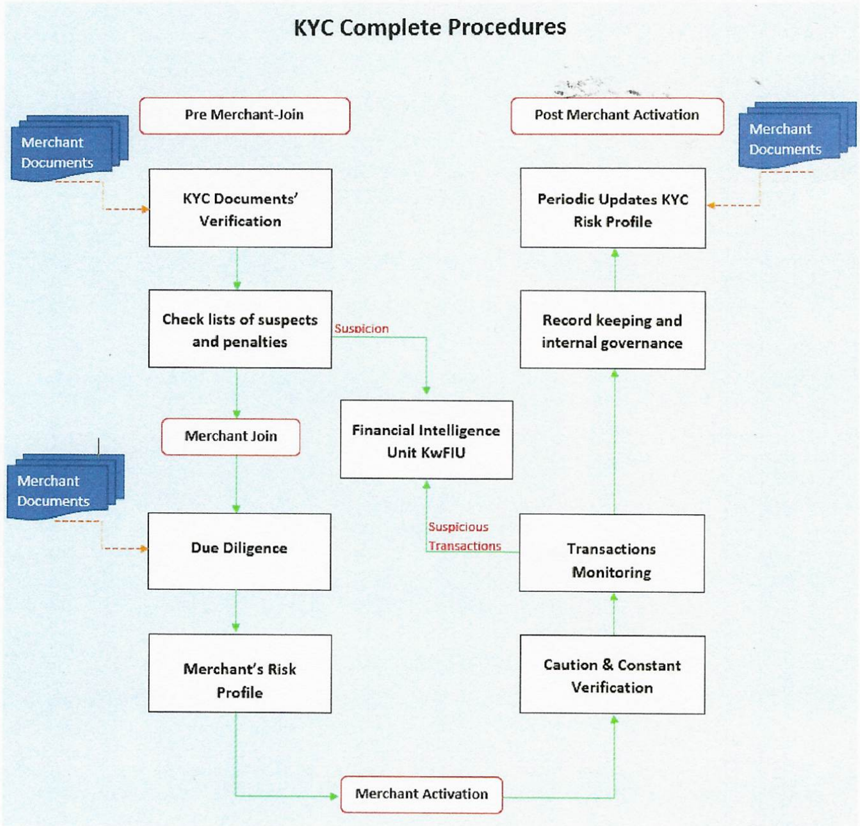
## Introduction

Automated Services Network Company is an electronic payment company and works on onboarding new merchants to its electronic services, so it needs to address some of the risks that arise, such as fraud, money laundering, etc. For this purpose, as well as regulatory guidelines and applicable laws require the adoption of several precautionary measures, including "Know Your Customer" and the merchant's due diligence procedures. We therefore conduct a practical set of verifications for these merchants, which begins before join us and continues until the end of his/her relationship with us.

## Know Your Customer KYC Definition

Regulated financial institutions such as banks, investment, and finance companies, etc., perform a "Know Your Customer" when a customer tries to open an account with them or join them (for example: the "Know Your Customer" process that you perform when opening a bank account). The customer may be an individual or a legal entity. The goal is to prove the customer's identity, address and legitimacy by verifying his main documents. In combination with due diligence and other mandatory checks, these checks identify potential fraudsters, shell companies, detect money laundering, etc. Unregulated entities, such as online marketplace companies for example, often need to perform a full or partial "know your customer" procedure as a precaution. These steps allow us to take a step towards not only securing our company, but also our end customers and the financial system as a whole.

As the company serves a different range of businesses, such as e-commerce markets, financial services such as lending/wealth management/credit management/payments/insurance, educational tech, health technology, digital entertainment and streaming services such as video/music/games, subscriptions such as SaaS companies and hospitality/transportation services such as taxi fees collectors/hotel booking collectors/vehicle rentals, etc., and therefore the checks we carry out vary from one company to another, especially based on the legal form of the merchant and the field of business.




## Merchant Onboarding Procedures – KYC & Risk Assessment

Based on the directions of the Central Bank of Kuwait, Law No. 106 of 2013 on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), and FATF recommendations, the company follows the below structured process for onboarding merchant.

The company is committed to the provisions of Circular No. 2/105/2209/2025 regarding Resolution No. 8 of 2025, issued on March 16, 2025, concerning the Executive Regulations for implementing the Security Council resolutions issued under Chapter VII of the United Nations Charter related to the fight against terrorism and the financing of the proliferation of weapons of mass destruction.

**The company is committed to the resolution concerning:**

- Immediate and prompt compliance with the decisions issued by the sanction committees of the Security Council, as well as decisions aimed at preventing and disrupting terrorism or its financing.
- Providing the Central Bank of Kuwait with all available data and information through the email addresses we have.

**Mechanism for Implementing Decision No. (8) of 2025 Regarding Security Council Resolutions, Requiring Financial Institutions to Implement Security Council Decisions Issued Under Chapter VII:**

- Verify customers against international sanctions lists (UN Sanctions Lists) as Advanced screening search - OpenSanctions, Sanctions List Search, .
- Immediately freeze assets without prior notice upon a match.
- Notify relevant authorities such as the Financial Intelligence Unit and the Central Bank.

- Maintain accurate records of the actions taken for ten years as stipulated in the Ministry of Commerce regulations.
- Regularly update databases to ensure ongoing compliance.

## Step 1: Document Inspection or Customer Screening Process (KYC)

The first stage is the examination of KYC documents or the Due Diligence of Customer Diligence ("CDD") process. It can be one or more of the following formats KYC for individuals and KYC for business

**Know Your Customer for Individuals**: When there is an individual merchant (example: a sole proprietary), we carry out a "Know Your Customer" process or prior customer investigations. Broadly, we verify the identity of an individual via a "valid official document" or an Official Valid Document OVD check such as civil ID documents, or passport, etc. And check business type, foundation date, business place, etc. We can also request further documents to check the financial/business status, for example, (commercial register, foundation contract).

**Know Your Customer for Businesses**: When it comes to commercial companies, we implement a "Know Your Customer" or "CDD" process for businesses. The Officially Valid Documents verification method is started by the "Proof of Entity" method. This varies based on the legal type of entity:

- **Enterprises**: Certificate of incorporation, memorandum, articles of association, etc.
- **Partnerships**: Partnership contract, registration certificates, etc.
- **Authorized Representatives:** Verified through board resolutions, power of attorney, etc.

Additionally, a beneficial ownership check is conducted to verify actual owners/controllers (directors,

- **Complex Ownership Structures:** Additional verification steps to trace UBOs through all layers.
- **Non-Resident Customers:** Enhanced scrutiny for entities or individuals based outside Kuwait.
- **Special Purpose Vehicles (SPVs), Trusts, Opaque Entities:** Enhanced documentation to validate purpose and legitimacy.
- **Geographic Risk:** Customers linked to high-risk or sanctioned jurisdictions (FATF grey/blacklists) will be flagged and subject to enhanced due diligence.

**Procedures for Verifying the Beneficial Owner of Legal Entities:**
The beneficial owner is the person who owns or effectively controls the legal entity, and can be identified through the following methods:

- **Requesting Documents**: Requiring documents that prove ownership and control (e.g., shareholder registers or incorporate documents).
- **Verifying Information through Trusted External Sources**: Cross-referencing data with reliable external sources.
- **Updating Beneficial Owner Data**: Ensuring that any changes to the beneficial ownership are reflected and updated.
- **Maintaining Accurate Records**: Keeping detailed records for at least ten years.
- **Rejecting Transactions with Entities**: Refusing to deal with entities that do not provide sufficient information about the beneficial owner.

## Step 2: Check Sanctions Lists

Next, we need to check the names of our clients and beneficiary owners against certain lists, such as national and international terrorist lists, or "politically exposed persons" lists. If a name matches a sanctions list, we also need to report this to the Financial Intelligence Unit ("KwFIU"). In addition, we check many other lists, such as blacklists/grey lists/shortcoming lists of companies, directors, etc.

issued by banks, the Securities Markets Authority, the Bureau of Foreign Affairs and Asset Control (US) and Advanced screening search - Open Sanctions (https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists , https://www.opensanctions.org/advancedsearch/)etc. These checks help us in the fight against terrorism and money laundering, and also help us determine the risk levels of a particular client.

Sanctions lists and blacklists are reviewed, including:

- OFAC (Office of Foreign Assets Control).
- United Nations sanctions lists.
- Local laws, regulation, and rulings – all verified by the compliance Department.

**Reputation Check:**

Online reviews and any previous issues with other service providers are examined such as (bing.com, facebook.com, instagram.com, linkedin.com, google.com, twitter.com).

These screening are performed prior to onboarding to identify merchants' compliance.

**Negative Merchant Registry**

The company maintains an internal Negative Merchant Registry that captures:

- Merchants previously terminated by the company.
- Merchants rejected during the due diligence process for risk-related reasons.
- Entities linked to fraudulent, abusive, or non-compliant activities.
  Merchants listed in the internal registry are barred from reapplication or reactivation unless specifically cleared through a documented review process.
  The registry is maintained and regularly updated by the Compliance Department, with controlled access granted to relevant teams including Sales and Operations.

## Step 3: Setup Policies and Merchant Inspection Set up

Next, we conduct a merchant's background check and a precedent check, which takes the form of a preliminary check, for which we define the merchant's internal inclusion policy. Our goal here is to verify the nature, purpose and good faith of the prospect's business. We conduct a range of checks such as licensing/registration checks, credit checks, profit and loss statement checks, balance sheet reviews, etc., based on the information we request directly from the prospect, along with checking publicly available information such as merchant locations, product listings, end customer reviews, social media activity, etc. to ensure the legitimacy of the business. It is also checking the business compatibility with the required security levels in its infrastructure.

## Step 4: Merchant Identification and Risk Profiling

After these initial checks and due diligence, merchants are risk-classified as **Low, Medium, High, or Prohibited**.

**Risk Profiling Factors Considered:**

- Transaction profile (expected daily volumes, amounts, frequency).
- Ownership & legal structure complexity.

- Residency (resident vs. non-resident).
- Geographic exposure (links to high-risk/sanctioned countries).
- Nature of business (sector-specific risks).
- PEP status of owners or representatives.
- Reputation risk (adverse media, negative history).

**Risk Categories & Documented Due Diligence Measures:**

| Risk Level | Due Diligence Measures | Ongoing Monitoring |
|---|---|---|
| Low Risk | Standard KYC documents + sanctions screening | Annual review |
| Medium Risk | Standard KYC + enhanced ownership verification + financials + reputation check | Semi-annual review |
| High Risk | Enhanced KYC + UBO tracing + Senior management approval before onboarding | Quarterly review + continuous monitoring |
| Prohibited Sectors | Onboarding denied (gambling, hacking, adult content, weapons, etc.) | N/A |

The company applies the **Risk-Based Approach (RBA)** in full alignment with Law 106/2013, CBK instructions, and FATF standards.

## Step 5: Ongoing Due Diligence

After the preparation process is over, our backup checks continue to track any changes in merchant behavior that are cause for concern. For example, a change in merchant website details or an unexpected list of high-risk products may indicate fraud. These may also require a review of merchant risk profiles and required due diligence levels.

## Step 6: Monitor Transactions and investigations

One of the most important inspections we carry out is to monitor business transactions, to detect any possible red flags, such as differences in the characteristics of expected transactions. For example, the expected total volume of transactions, the expected number of transactions, the average order value, the frequency of chargebacks, etc., for example, if a merchant exceeds the maximum transaction allowable, observes an unusual refund pattern, or we receive several complaints from end customers - these are reasons for concern. In case of any suspicious transactions (e.g. raising concerns about money laundering) and also transactions exceeding certain thresholds, we report it to the Financial Intelligence Unit.

Among the procedures that have been put in place are the following:

- Setting a limit on the number of transactions and the total daily amounts of the merchant according to the nature of his/her work. A daily transaction report is issued and presented to the Executive Manager (merchant account manager), Compliance Officer and Compliance Officer Assistant. The report is also on the system for reference at any time.
- The transactions are monitored daily, and the customer's movement is evaluated, and in the event of suspicion of any operations, the service is stopped, and the transfer of the collected amounts is stopped until the merchant is contacted to provide the data of these suspicious transactions to ensure their correctness, and on the basis of them, measures

are taken to stop or resume the service with him/her. The report is also displayed in the system for reference at any time. The report displays operations done during the day from a single IP as well as operations that exceed a certain amount.

- The company only allows payment services through K-Net and Credit Card (locally)

In the event that any suspicious transactions of money laundering or transactions exceeding certain thresholds are detected or an unusual recovery pattern is observed, the Compliance Officer will suspend the service from the Merchant and inform the Merchant of the suspension to allow him/her to provide proof or supported documents of the transaction/s so that it would be legalized else eNet seizure of suspicious amounts and inform the Financial Intelligence Unit.

Ongoing transaction monitoring is performed by the company's automated system to:

- Track the merchant's daily transactions.
- Detect any suspicious or fraudulent activity.
- Identify potential money laundering or terrorist financing operations.

An update automated alert system is in place.

- A daily email notification is sent to:
    - The Accounting Department.
    - The Sales Department.
    - Compliance Department.
    - The General Manager.
- This alert is triggered when any transaction exceeds the client's allowed daily transfer limit. Periodic KYC updates are also performed.

- The update schedule is determined based on the client's risk assessment.

## Step 7: Merchant Website Verification & Online Presence Check:

As part of the Merchant Due Diligence process, the Compliance/Risk team shall conduct a thorough online presence and website verification to ensure the legitimacy and operational presence of the merchant. The following checklist outlines the key risk indicators and verification steps.

1. **Domain Verification**
    - Domain Consistency: Compare the domain with known official domains. Look for typo squatting (e.g., g00gle.com vs. google.com).
2. **SSL Certificate Check**
    - Ensure the website uses HTTPS certificate).
3. **Business Information Consistency**
    - Match the websites contact details (address, email, phone) with official record (e.g., business license, commercial registry).
    - Verify the business registration number with the relevant government authority (e.g., Ministry of Commerce in the country of registration).
4. **Cross-Check Against Known Lists**
    - Screen the domain and company name against:
        - Sanctions list (OFAC, UN, EU, etc.).
        - Negative media databases.
        - Internal blacklists.
5. **Technical Website Analysis**

- Use tools like google Safe Browsing, Virus Total to test for phishing, malware, or spoofing risks.

6. **Validate Ownership**
    - Ask for:
        - Business license tied to the domain name.
7. **Content Review**
    - Rreview grammar, formatting, and layout – poor quality can indicate a fake site.
8. **Background Checks**
    - Conduct a KYB **(Know Your Business**) review:
        - Get corporate documents.
        - Review beneficial ownership structure.
        - Verify authorized signatories.
9. **Third-Party References**
    - Look for company mention on:
        - LinkedIn (company profile).
        - Google Reviews, Bing etc.
        - Industry forums or local regulatory bodies.
10. **Red Flags to Watch**
    - No social media presence or fake-looking profiles.
    - Unverifiable physical address.
    - Contact only via web forms or personal emails (e.g., Gmail).
    - Promises of guaranteed returns or unrealistic offers.

## Step 8: Record Keeping and Internal Governance Requirements

After that, we keep records of all merchant transaction and identification documents, usually for at least 10 years. These must be submitted to authorities upon request, such as an investigation. There are requirements, such as ad internal committees, internal audits, periodic risk assessments, and appropriate staff training.

## Step 9: Customer acceptance and Onboarding process:

1- **Document Collection (Sales Department):**
- The Sales Department collects all required documents from the merchant as per the list provided in **step1.**
- A checklist is used to ensure completeness before proceeding.

2- **Initial Review (Compliance Officer):**
- Documents and merchant information are reviewed by the Compliance officer to verify:
    - Accuracy and completeness of the submitted documents.
    - Screening against internal and external sanctions/blacklists.
    - Risk scoring.

3- **System Upload & Request for Approval:**
- Sales uploads the verified documents into the merchant onboarding system.
- An approval request is triggered for the Compliance Department.

4- **Compliance Approval:**

- The Compliance Officer performs a final review and gives formal approval.
- If any issue is identified, the merchant is flagged and returned to Sales for correction or rejection.

5- **Merchant ID (MID) Generation:**
- Upon approval, the system automatically generates a **MERCHANT ID (MID).**
- **The merchant's status in the system is updated to "Approved"**

6- **Post-Approval Actions:**
- **Accounting/Finance Department:** Confirms and configures the settlement cycle and fee structure as per the agreement.
- **IT Department:** Grants access to the Merchant Dashboard and sets up user credentials.
- A dedicated merchant system profile is created in coordination with relevant departments.

7- **Confirmation to Merchant:**
- A formal welcome email or notification is sent to the merchant with access credentials, MID, and onboarding confirmation.

8- **Merchant Category Code:**
We utilize the Merchant Category Code (MCC) to classify transaction, ensuring that only categories permitted under Kuwait law are accepted.
**Accepted Merchants as per MCC:**
- **(Agricultural Services).**
- **(Contracted Services).**
- **(Transportation Service).**
- **(Utility Services)**
- **(Retail Outlet Services).**
- **(Clothing Stories).**
- **(Business Services).**
- **(Professional Services and Membership Organizations).**
- **(Government Service).**
- **(Travel and Entertainment).**
- **(Airlines).**
- **(Car Rental).**
- **(Lodging).**

**The Prohibited list of merchant categories**

These categories are explicitly banned under Kuwaiti law or by payment processors operating in the country:

- **Online Gambling and Betting:** Including casinos, lottery tickets, and wagers.
- **Pornography and Adult Content:** Website or services promoting adult content or escort services.
- **Cryptocurrency Exchanges:** Platforms facilitating the buying, selling, or trading of cryptocurrencies.
- **Telemarketing and Outbound Sales:** Direct marketing services, especially those involving unsolicited calls or emails.

- **Money Transfer Services:** Including wire transfers and money orders.
- **Pharmacies and Drug Stores:** Online sale of pharmaceuticals or drug-related products.
- **Dating and Escort Services:** Platforms offering dating services or escort-related content.

**High-risk merchant categories**

These categories are not outright banned but are subject to heightened scrutiny and may face higher fees or stricter compliance requirements:

- **Travel Agencies and Tour Operators:** Due to potential chargebacks and fraud risks.
- **Telecommunication Services:** Including telecom equipment sales and services.
- **Direct Marketing and Subscription Services:** Especially those involving continuity billing or catalogue sales.
- **Timeshare Sales:** Involving the sale or rental of timeshare properties.
- **Cigar Stores and Stands:** Selling tobacco products.
- **Video Game and Arcade Services:** Particularly those involving skill-based wagering.
- **Foreign Currency and non-Fiat Currency Services:** Including cryptocurrency transactions.

## Step 10: Procedures for Terminating or Suspending the Merchant Service:

The transactions are monitored daily, as well as the expiry dates of the merchants supporting documents, and the customers transactions are monitored, and in the event of suspicion of any operations or the expiration of any document without the merchant providing the document to the company after updating it, the service is suspended and the transfer of the collected amounts is stopped until the merchant is contacted to submit the required updated document or data of those suspicious operations to ensure their correctness, and on the basis of them, measures are taken to stop or resume the service with him/her. The procedures for terminating the relationship or suspending the service the company's merchants and settling the amounts related to it shall be determined **for one of the following reasons:**

1. Expiry of any supporting document without the merchant providing the updated document to the company.

   **Action Taken:**

   - The merchant shall be notified of the company's desire to terminate the service with him within one working day with an explanation of reason.
   - The Executive Manager sends an email to both the accountant and the compliance Officer to stop the service.
   - The Compliance Officer stops the service through the system.
   - The Accounting Department settles any dues to the merchant to transfer them on the next day.
   - The merchant is notified of the suspension/termination of the service with the statement of dues by e-mail.

2. Violation of any of the laws or regulations in force in the State of Kuwait.
3. Using the service for illegal activities.
4. Violation of the nature work activity.

   **Action Taken:**

- The merchant shall not be notified of the company's desire to terminate the service with him.
- The Executive Manager sends an email to both the accountant and the compliance Officer to stop the service, freeze the settlement.
- The Compliance Officer stops the service through the system and report the issue to KWFIU.

## Step 11: Periodic Updates:

The company ensures that merchant risk profiles and "Know Your Customer" information are kept up to date based on their assigned risk rating:

- Low Risk (Score 1): Update every three years.
- Medium Risk (Score 2): Update every two years.
- High Risk (Score 3): Update annually.

These updates include refreshing KYC documents, re-checking beneficial ownership, sanctions/PEP screening, and reviewing transaction patterns to identify changes in risk exposure.

**Ongoing Due Diligence:**

- Continuous monitoring is applied to all merchants to identify unusual or suspicious activity.
- Adverse media, sanction list updates, and changes in ownership/structure are tracked and reflected in the merchant risk profile.
- Any material changes trigger an immediate KYC refresh regardless of the scheduled periodic review.