KYC360
A part of experian.

KYC / AML Requirements

By Entity Type

Individuals

- Proof of identity
- Personal information
- Purpose and expected activity
- Authority (where applicable)

Corporations

- Formation and registration evidence
- Address
- Ownership structure and UBO identification
- Directors and authorised signatories
- Service providers
- Business activity and purpose
- Source of funds/wealth

Partnerships

- Partnership agreement/deed
- General Partner (GP) and controllers
- Limited Partners (LPs)/partners and beneficial owners
- Evidence of ownership/control
- Purpose and funding

Trusts

- Trust deed and amendments
- Trust parties
- Control and authority
- Source of funds/wealth
- Ongoing updates

Foundations

- Charter/founding documents
- Structure and key persons
- Authority
- Source of funds/wealth

Funds

- Fund structure documentation
- Controllers and operators
- Investor approach (risk-based)
- Purpose and expected flows
- Source of funds/wealth

Estates

- Proof of death and authority
- Executor/administrator
- Beneficiaries
- Nature of assets and expected flows

NBFIs

- Licensing/registration
- Full KYB
- Business model and expected activity
- Regulatory history (risk-based)
- Enhanced measures (risk-based)

General Requirements (All Entity Types)

1.Risk-Based Approach

KYC/AML controls must be proportionate to risk. The same checks that are appropriate for a low-risk retail customer will not be sufficient for a complex, cross-border structure or a customer linked to higher-risk industries and geographies.

2.Customer Identification

Identify the customer using core data (names, dates, addresses, registration details, identifiers) and verify those details with reliable evidence.

3.Certification (Electronic and Wet-Ink)

FATF aligned jurisdictions have permitted electronic certification and digital identification, including online biometric checks, to verify customer identities and supporting documents. These checks must be aligned to regulatory requirements and support a risk-based approach.

4.Ownership and Control

Identify the natural persons who ultimately own/control the customer and understand the ownership and control structure.

5.Structure Charts

Structure charts should be obtained whenever there is complexity, layering, cross-border ownership, trustees/foundations, nominee roles, multiple share classes, or non-obvious control.

6.Screening

Screen the customer and relevant connected parties for:

- Sanctions and watchlists
- PEP status
- Adverse media (risk-based, especially for higher-risk customers and when negative information could affect the risk assessment)

7.Source of Funds and Source of Wealth

Source of funds and wealth checks should support a credible, evidence-based understanding of how money enters and moves through the relationship.

8.Enhanced Due Diligence

Higher-risk customers, such as those identified as PEPs or where there is exposure to high-risk jurisdictions. require stronger measures. Typical enhancements include deeper independent corroboration, stronger funds/wealth evidence, clearer rationale for complexity, senior approvals for onboarding (common for PEP risk), tighter monitoring, and more frequent reviews.

9.Ongoing Monitoring and Refresh

Ongoing monitoring tests whether activity matches the expected profile established at onboarding. KYC refresh keeps information current as customers change (ownership updates, new controllers, new products/geographies, new negative information).

10.Record-Keeping and Governance

Maintain a defensible audit trail of what was collected, how it was verified, and why risk decisions were made. Ensure policies, procedures, training, QA, escalation routes, and reporting controls are in place. Regulators often require records to be kept for at least 5 years after a customer has been offboarded.

/ Full cycle Onboarding, Screening and CLM at the speed of business