

KYC Checklist: 10 Essential Steps for Compliance Success

Use this checklist to standardize your KYC/AML processes. Add notes for audit trails.



1. Customer Onboarding and Data Collection

Collect core customer details (name, DOB, address, government ID).

Use standardized digital forms to reduce errors.

Verify completeness of submitted information.

Notes:

2. Identity Verification and Authentication

Validate documents manually and/or with automated tools.

Check for expiration dates, authenticity, and cross-database matches.

Use OSINT tools like **ShadowDragon Horizon™** to corroborate identity data with public information and detect impersonation or synthetic IDs.

Record verification method used.

Notes:

3. Sanctions and PEP Screening

Screen against global watchlists (OFAC, UN, EU, etc.).

Identify Politically Exposed Persons (PEPs).

Apply Enhanced Due Diligence (EDD) when necessary.

Use **ShadowDragon Horizon™** to reveal indirect or hidden associations with sanctioned or politically exposed networks not found in static lists.

Notes:

4. Risk Assessment and Profiling

Assign risk scores based on geography, occupation, and behavior.

Document Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) cases.

Use a standardized scoring matrix for consistency.

Incorporate OSINT-driven behavioral and reputational signals (e.g., adverse media, online activity) from ShadowDragon to refine CDD/EDD scoring.

Notes:

5. Beneficial Ownership Identification

Identify Ultimate Beneficial Owners (UBOs).

Verify ownership charts and supporting documents.

Maintain records to comply with regulatory thresholds.

Map relationships between entities and individuals with **ShadowDragon Horizon™** to detect concealed or cross-border ownership ties.

Notes:

6. Ongoing Monitoring and Transaction Alerts

Set periodic review cycles based on customer risk.

Update customer data upon changes (e.g., job, jurisdiction, suspicious activity).

Retrain risk models regularly to avoid drift.

Use **Horizon™ Monitor** for continuous OSINT collection to identify emerging risks (e.g., new associates, shell entities, or online activity shifts).

Notes:

7. Ongoing Monitoring and Transaction Alerts

Store all customer records securely for 5-7 years.

Ensure accessibility for audits while maintaining encryption and access controls.

Back up records regularly. (ShadowDragon automatically preserves source data, investigative steps, and timestamps, ensuring a verifiable audit trail.)

Notes:

8. Reporting Suspicious Activity

- Define internal escalation and SAR filing procedures.
- Train staff on how and when to file Suspicious Activity Reports.
- File SARs within required regulatory timelines.

Notes:

9. Employee Training and Awareness

- Conduct mandatory, role-specific KYC/AML training annually.
- Provide refreshers when regulations change.
- Verify staff proficiency with compliance tools.
- Include **OSINT best practices** and ShadowDragon workflows in training to ensure analysts understand lawful, ethical intelligence collection

Notes:

10. Independent Audit & Program Review

- Schedule annual internal/external audits.
- Review audit findings and implement corrective actions.
- Document improvements for future reviews.

Notes:

Integrate OSINT and leverage tools like **ShadowDragon Horizon™** across these steps to strengthen KYC, improve audit readiness, and maintain proactive risk visibility.



SHADOWDRAGON