International Anti Money Laundering Standards

Customer Due Diligence Procedures

Adverse Media – negative press, reputational risk
A source of information that may indicate a customer’s involvement in illicit activities, including newspaper articles, online reports, and regulatory filings. Financial institutions scan adverse media during the CDD onboarding process to identify potential red flags.
Example: A news article linking a corporate client to a known smuggling network triggers a deeper investigation.
Practical application: Integrate automated media monitoring tools with the client onboarding workflow to flag adverse media in real time.
Challenges: Differentiating between unverified rumors and substantiated allegations; managing language barriers and jurisdictional differences in media coverage.

Beneficial Owner – ultimate controller, ownership structure
The natural person who ultimately owns or controls a legal entity, either directly or indirectly, typically through ownership of at least 25 % of the voting rights or through other means of control. Identifying the beneficial owner is a core element of CDD to prevent the use of opaque structures for money laundering.
Example: A limited liability company is owned 30 % by Person A, 30 % by Person B, and the remaining shares are held by a trust; Person A and Person B are the beneficial owners.
Practical application: Use corporate registry data, shareholder registers, and trust deed analysis to map ownership layers.
Challenges: Complex corporate structures, nominee shareholders, and jurisdictions with limited public disclosure impede accurate identification.

Customer Identification Program (CIP) – verification, KYC, onboarding
A set of procedures that obligates a financial institution to collect and verify the identity of each customer before establishing a business relationship. CIP requirements are mandated by international AML frameworks such as the FATF Recommendations and the EU’s AML Directives.
Example: Collecting a passport, proof of address, and a government-issued tax identification number for a new retail client.
Practical application: Deploy electronic identity verification (eIDV) solutions to accelerate the CIP while maintaining compliance.
Challenges: Balancing speed of onboarding with thoroughness; handling customers lacking conventional identification documents.

Enhanced Due Diligence (EDD) – high-risk, additional scrutiny
A heightened level of CDD applied to customers or transactions that present a higher risk of money laundering or terrorist financing. EDD involves gathering more detailed information, conducting ongoing monitoring, and sometimes obtaining senior management approval before proceeding.
Example: A politically exposed person (PEP) opening a high-value corporate account triggers EDD,

requiring source-of-wealth documentation and senior approval.
Practical application: Develop risk-based EDD checklists that specify required documentation, approval workflows, and review frequency.
Challenges: Determining the appropriate threshold for EDD; ensuring that additional documentation does not become a barrier to legitimate business.

Financial Action Task Force (FATF) – global standard-setter, AML/CTF
An inter-governmental body that formulates international standards to combat money laundering, terrorist financing, and proliferation financing. FATF's 40 Recommendations form the backbone of most national AML regimes, including requirements for CDD.
Example: A jurisdiction that fails to implement FATF-mandated CDD measures may be placed on the FATF "gray list," leading to higher scrutiny from correspondent banks.
Practical application: Align internal CDD policies with FATF's "risk-based approach" to demonstrate compliance during supervisory examinations.
Challenges: Keeping pace with FATF's evolving guidance, such as the 2022 update on virtual assets and crypto-related businesses.

Geographic Risk Assessment – jurisdictional risk, country rating
The process of evaluating the money-laundering risk associated with a particular country or region based on factors such as corruption levels, prevalence of illicit financial activities, and regulatory effectiveness. Geographic risk informs the level of CDD required for customers linked to high-risk locations.
Example: A client operating in a jurisdiction with a "high" FATF rating will be subject to stricter CDD controls than a client in a "low" risk country.
Practical application: Maintain an up-to-date country risk matrix and integrate it into the client risk-scoring engine.
Challenges: Rapid changes in political or regulatory environments can render static risk matrices outdated.

High-Risk Customer – risk rating, monitoring
A client whose profile, transaction pattern, or affiliation (e.g., PEP, offshore entity, high-value cash transactions) suggests a greater likelihood of involvement in money laundering or terrorist financing. High-risk customers require intensified CDD, continuous monitoring, and periodic review.
Example: A private-wealth client who conducts frequent large-value wire transfers to jurisdictions with weak AML controls.
Practical application: Assign dedicated relationship managers and implement real-time transaction monitoring thresholds tailored to the client's risk level.
Challenges: Avoiding "risk fatigue" where analysts become desensitized to alerts due to high volume.

Identification Documents – primary ID, secondary ID
Official documents used to verify a customer's identity, such as passports, national ID cards, driver's licences, and utility bills. International standards require that at least one primary document be government-issued and that secondary documents corroborate address or birth-date information.
Example: A passport provides the primary ID; a recent electricity bill serves as the secondary proof of residence.

Practical application: Create a document-acceptance matrix that lists acceptable primary and secondary documents per jurisdiction.
Challenges: Counterfeit documents, document expiration, and customers from jurisdictions with limited issuance standards.

International Sanctions Lists – OFAC, UN, EU, screening
Compilations of individuals, entities, and regimes that are subject to economic or trade restrictions imposed by governments or international bodies. CDD procedures must include screening against these lists to prevent prohibited transactions.
Example: A client's beneficial owner appears on the United Nations "terrorist list," resulting in account denial.
Practical application: Deploy automated sanctions-screening engines that perform fuzzy matching and provide audit trails for hits.
Challenges: Managing false positives, updating lists in real time, and dealing with divergent naming conventions across jurisdictions.

Know Your Customer (KYC) – client verification, onboarding
A collective term for the processes and controls used by financial institutions to verify the identity of their clients, assess risk, and maintain up-to-date information throughout the relationship. KYC is the practical implementation of CDD within day-to-day banking operations.
Example: Collecting identification, conducting risk scoring, and storing the client profile in a secure database.
Practical application: Integrate KYC workflows with the institution's CRM system to ensure seamless data flow and auditability.
Challenges: Keeping KYC data current as client circumstances evolve, especially for corporate clients with frequent ownership changes.

Legal Entity Identifier (LEI) – global identifier, GLEIF
A 20-character, alpha-numeric code that uniquely identifies legally distinct entities that engage in financial transactions. LEIs facilitate transparency in the corporate ownership chain and are increasingly required in CDD for corporate clients.
Example: A multinational corporation provides its LEI during account opening, enabling the bank to retrieve its publicly disclosed ownership information.
Practical application: Use the Global Legal Entity Identifier Foundation (GLEIF) API to automatically retrieve and store LEI data during onboarding.
Challenges: Incomplete LEI coverage in certain jurisdictions and the need to reconcile multiple LEIs for complex group structures.

Money Laundering – placement, layering, integration
The process by which illicit proceeds are disguised as legitimate funds through a series of financial transactions. The three classic stages—placement, layering, and integration—guide AML risk assessments and CDD focus areas.
Example: Cash from illegal drug sales is deposited (placement), transferred through multiple offshore

accounts (layering), and finally invested in a legitimate real-estate project (integration).
Practical application: Design CDD controls that detect anomalies at each stage, such as unusually large cash deposits or rapid movement of funds across borders.
Challenges: Sophisticated laundering techniques, including the use of virtual assets and trade-based schemes, require continuous adaptation of detection methods.

Non-Financial Business and Professions (NFBP) – lawyers, accountants, real estate
Sectors that, while not traditional financial institutions, are vulnerable to money-laundering abuse because they handle client funds or facilitate transactions. Many jurisdictions extend CDD obligations to NFBPs, requiring them to implement similar risk-based controls.
Example: A law firm that holds client escrow funds must conduct CDD on the underlying beneficial owners.
Practical application: Provide sector-specific CDD guidelines and training to NFBP clients, emphasizing record-keeping and reporting duties.
Challenges: Varied regulatory expectations across jurisdictions and limited resources within smaller NFBP firms.

Officer, Director, and Senior Manager (ODSM) Screening – UBO, corporate governance
The practice of screening not only the beneficial owners of a corporate client but also its key officers, directors, and senior managers for sanctions, PEP status, or adverse media. ODSM screening expands the risk view beyond ownership percentages.
Example: A director of a client company is identified as a PEP, prompting the bank to apply EDD to the entire corporate relationship.
Practical application: Create automated workflows that extract ODSM data from corporate filings and feed it into the sanctions-screening engine.
Challenges: Keeping ODSM data current, especially when changes are not publicly disclosed promptly.

Politically Exposed Person (PEP) – public official, risk factor
An individual who holds or has held a prominent public function, as well as immediate family members and close associates. PEPs are considered higher-risk customers due to the potential for corruption and abuse of public office.
Example: A senior minister who opens a personal bank account is classified as a PEP.
Practical application: Apply a PEP risk matrix that defines additional documentation (e.g., source-of-wealth statements) and higher-frequency transaction monitoring.
Challenges: Identifying indirect connections, such as family members residing abroad, and handling political changes that affect PEP status.

Risk-Based Approach (RBA) – proportionality, assessment
A methodology that tailors CDD measures to the level of risk presented by a customer, product, service, or geographic factor. The RBA is a cornerstone of FATF guidance, requiring institutions to allocate resources where they are most needed.
Example: Low-risk retail customers may undergo simplified CDD, while high-risk corporate clients receive full EDD.

Practical application: Implement a risk-scoring engine that aggregates quantitative and qualitative data to produce a risk rating for each client.
Challenges: Ensuring that risk models are transparent, auditable, and periodically recalibrated to reflect emerging threats.

Screening – match, false positive, watchlist
The process of comparing client data against various watchlists (sanctions, PEP, adverse media) to detect potential matches that require investigation. Effective screening balances thoroughness with operational efficiency.
Example: An automated system flags a client name that closely resembles a sanctioned individual, prompting a manual review.
Practical application: Use fuzzy-matching algorithms and tiered escalation procedures to manage alerts.
Challenges: High false-positive rates can overwhelm compliance teams; linguistic variations and transliteration issues increase complexity.

Source-of-Wealth (SOW) Declaration – wealth origin, documentation
A statement, often accompanied by supporting evidence, that explains how a customer acquired the funds used in a particular transaction or account. SOW is distinct from “source-of-funds,” which relates to a specific transaction; SOW looks at the broader wealth accumulation.
Example: A client provides audited financial statements, inheritance documents, and tax returns to substantiate a $5 million deposit.
Practical application: Require SOW documentation for high-value accounts and retain it for the statutory retention period.
Challenges: Verifying the authenticity of supporting documents and assessing the plausibility of declared wealth narratives.

Transaction Monitoring – behavioral analytics, alerts
The ongoing surveillance of customer transactions to identify patterns that deviate from the expected behavior profile, potentially indicating money-laundering activity. Monitoring systems generate alerts that are investigated by analysts.
Example: A corporate client suddenly initiates a series of high-value wire transfers to a new set of offshore beneficiaries, triggering an alert.
Practical application: Deploy machine-learning models that adapt to evolving transaction patterns and reduce false positives over time.
Challenges: Balancing detection sensitivity with operational workload; integrating monitoring across multiple channels (payments, securities, trade).

Ultimate Beneficial Owner (UBO) – direct, indirect control
The natural person who ultimately owns or controls a legal entity, often distinguished from intermediate shareholders. UBO identification is crucial for uncovering hidden ownership structures used to conceal illicit activity.
Example: A trust holds shares in a company; the settlor of the trust is the UBO because they retain control over the trust assets.

Practical application: Use a hierarchical ownership mapping tool to trace ownership chains back to the UBO level.
Challenges: Jurisdictions that allow nominee shareholders or opaque trusts impede accurate UBO discovery.

Virtual Asset Service Provider (VASP) – cryptocurrency exchange, AML
An entity that conducts activities such as exchange between virtual assets and fiat currency, custody, or transfer of virtual assets on behalf of customers. International AML standards now require VASPs to implement CDD similar to traditional financial institutions.
Example: A crypto exchange must verify the identity of users, monitor transaction patterns, and report suspicious activity.
Practical application: Integrate blockchain analytics tools that trace the flow of tokens and flag suspicious patterns.
Challenges: Pseudonymous nature of blockchain addresses, rapid emergence of new token types, and regulatory fragmentation across jurisdictions.

Watchlist – sanctions, PEP, adverse media
A compiled list of individuals, entities, or vessels that are subject to regulatory restrictions or heightened scrutiny. Watchlists are used in screening processes to detect prohibited or high-risk counterparties.
Example: The OFAC SDN List is a watchlist that blocks U.S. persons from dealing with listed entities.
Practical application: Schedule daily updates of watchlist data feeds and automate the ingestion into the screening engine.
Challenges: Maintaining data quality, handling duplicate entries, and accommodating variations in naming conventions across sources.

Wire Transfer Monitoring – cross-border, SWIFT, red flags
A specialized subset of transaction monitoring focused on electronic funds transfers, particularly those that cross international borders via networks such as SWIFT. Wire transfers are a common conduit for layering illicit funds.
Example: A series of rapid, same-day transfers to a high-risk jurisdiction with no apparent business rationale raises a red flag.
Practical application: Set up rule-based triggers that consider origin, destination, frequency, and amount thresholds specific to wire activity.
Challenges: Real-time detection versus batch processing, handling large volumes of low-value transfers, and deciphering legitimate trade-based transactions.

AML Compliance Officer (ACO) – responsibility, oversight
The senior individual within a financial institution responsible for establishing, maintaining, and enforcing AML and CDD policies. The ACO ensures that the firm meets regulatory expectations and serves as the primary liaison with supervisors.
Example: The ACO signs off on the annual AML risk assessment and approves any exceptions to standard CDD procedures.
Practical application: Provide the ACO with dashboards that summarize key risk indicators, pending alerts,

and audit findings.
Challenges: Keeping abreast of regulatory changes, managing cross-departmental responsibilities, and securing adequate resources for compliance functions.

Anti-Money-Laundering (AML) Framework – policy, procedures, governance
The comprehensive set of policies, procedures, controls, and governance structures that an organization implements to prevent, detect, and report money-laundering activities. The AML framework incorporates CDD as a foundational component.
Example: An AML framework includes a risk assessment, KYC onboarding, transaction monitoring, reporting mechanisms, and training programs.
Practical application: Conduct periodic internal audits to evaluate the effectiveness of each AML component and remediate identified gaps.
Challenges: Ensuring consistency across global business units and integrating legacy systems into a unified compliance architecture.

Risk Rating – score, tier, categorization
A numerical or categorical value assigned to a customer, product, service, or geography that reflects its assessed money-laundering risk. Risk ratings drive the intensity of CDD measures and ongoing monitoring.
Example: A client may be assigned a “high” risk rating based on a combination of PEP status, high-value cash deposits, and operation in a high-risk jurisdiction.
Practical application: Store risk ratings in the client master file and automate the selection of appropriate CDD templates based on the rating.
Challenges: Preventing rating inflation, ensuring that rating updates are triggered by changes in customer behavior, and aligning ratings with supervisory expectations.

Source-of-Funds (SOF) Verification – transaction-specific, documentation
The process of confirming the origin of money used in a particular transaction, distinct from the broader SOW analysis. SOF verification is required for large or unusual transactions to ensure they are not proceeds of crime.
Example: A client submits a bank statement showing the receipt of a loan that funds a $2 million wire transfer.
Practical application: Request and retain supporting documents such as loan agreements, sale contracts, or inheritance certificates for each flagged transaction.
Challenges: Matching documentation to the exact transaction, verifying the legitimacy of third-party sources, and handling cross-border fund flows.

Transaction Threshold – trigger, limit, monitoring
A predefined monetary value that, when exceeded, initiates additional scrutiny, such as enhanced monitoring or mandatory reporting. Thresholds are set based on regulatory requirements and internal risk appetite.
Example: Transactions above $10,000 require filing a Currency Transaction Report (CTR) in many jurisdictions.
Practical application: Configure the monitoring system to automatically flag transactions that surpass the

threshold and route them to the compliance team.
Challenges: Avoiding “threshold gaming” where customers split amounts just below the limit, and adjusting thresholds for inflation or market changes.

Travel Rule – information sharing, FATF
A requirement that financial institutions transmit certain originator and beneficiary information when conducting wire transfers above a specified amount, facilitating downstream AML investigation. The Travel Rule is part of FATF’s standards for both traditional banks and VASPs.
Example: When a bank sends a $25,000 SWIFT payment, it must include the sender’s name, address, and account number, as well as the beneficiary’s details.
Practical application: Implement a data-capture module that automatically populates the required fields for each outbound transfer.
Challenges: Interoperability between different messaging standards, data privacy concerns, and ensuring that legacy systems can embed the required information.

Transaction Pattern Analysis – behavioural profiling, anomaly detection
The analytical technique of examining a customer’s historical transaction data to establish a baseline of normal activity, then identifying deviations that may indicate illicit behavior. Pattern analysis underpins many modern AML monitoring solutions.
Example: A retail client who historically makes low-value purchases suddenly initiates a series of large cash deposits, signaling a possible shift in activity.
Practical application: Use clustering algorithms to group similar transaction behaviours and apply statistical thresholds for outlier detection.
Challenges: Data quality issues, the need for sufficient historical data, and the risk of over-fitting models to past patterns.

Unstructured Data in CDD – social media, news feeds, NLP
Information that does not conform to a predefined data model, such as free-text news articles, social-media posts, or PDF documents. Extracting relevant risk signals from unstructured data enhances CDD accuracy.
Example: Natural-language-processing (NLP) tools scan a news article mentioning a client’s involvement in a fraud investigation, flagging it for review.
Practical application: Deploy text-mining pipelines that convert unstructured sources into structured risk indicators for integration with the client risk profile.
Challenges: Language diversity, false positives from ambiguous phrasing, and the computational cost of large-scale text analysis.

Virtual Asset Transaction Monitoring – blockchain analytics, AML
The specialized monitoring of transactions involving cryptocurrencies, tokens, and other digital assets, using blockchain data to trace fund flows and identify suspicious patterns.
Example: A wallet address that receives funds from multiple high-risk jurisdictions and then transfers them to a mixing service triggers an alert.
Practical application: Integrate blockchain-explorer APIs and address-risk scoring services into the AML monitoring platform.

Challenges: Rapidly evolving token standards, privacy-enhancing technologies (e.g., mixers, privacy coins), and the lack of universal KYC at the protocol level.

Wire Transfer Reporting Obligations – CTR, SAR, jurisdictional
Legal duties that require financial institutions to report certain wire transfers to regulatory authorities, either as routine transaction reports (e.g., CTR) or as suspicious activity reports (SAR) when illicit intent is suspected.
Example: A bank files a SAR after detecting a series of transfers to a sanctioned country that lack a legitimate business purpose.
Practical application: Embed reporting triggers within the transaction monitoring system to generate pre-filled report templates for compliance review.
Challenges: Determining the appropriate threshold for filing, protecting confidentiality, and managing cross-border reporting coordination.

Zero-Risk Assumption – myth, compliance reality
The erroneous belief that a financial institution can completely eliminate money-laundering risk through extensive controls. International standards emphasize that risk can be mitigated, not eradicated, and that ongoing vigilance is required.
Example: Assuming that a client from a low-risk jurisdiction presents no AML concerns and forgoing periodic reviews.
Practical application: Reinforce a culture of risk awareness through regular training and internal communications that stress the dynamic nature of AML risk.
Challenges: Combating complacency, especially in mature markets, and allocating resources proportionally to residual risk levels.