Customer Due Diligence

Enhanced Due Diligence Unit

Anti-Money Laundering (AML) – A set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income. Related: CDD, KYC, SAR. AML programs require financial institutions to monitor transactions, report suspicious activity, and maintain records that help law-enforcement agencies trace illicit money flows.

Beneficial Owner – The natural person who ultimately owns or controls a client, even if the ownership is exercised through a chain of legal entities. Related: UBO, Transparency Register. Identifying the beneficial owner is essential for risk assessment, especially in high-risk jurisdictions where ownership structures may be opaque.

Compliance Officer – An individual appointed by a financial institution to oversee the implementation of AML/CFT policies, ensure adherence to regulatory requirements, and act as a liaison with supervisory authorities. Related: AML Officer, Risk Manager. The officer conducts training, reviews internal controls, and coordinates investigations of potential violations.

Customer Due Diligence (CDD) – The process of collecting and verifying information about a client's identity, business activities, and risk profile before establishing a business relationship. Related: KYC, EDD, Risk Assessment. CDD is the baseline level of scrutiny; it may be enhanced for higher-risk customers.

Enhanced Due Diligence (EDD) – A deeper level of investigation applied to customers or transactions that present a higher risk of money laundering or terrorist financing. Related: CDD, Risk-Based Approach. EDD involves gathering additional documentation, conducting source-of-funds analysis, and performing ongoing monitoring at a higher frequency.

Enhanced Due Diligence Unit (EDDU) – A specialized team within a financial institution tasked with executing the EDD process for high-risk customers, complex transactions, and politically exposed persons. Related: EDD, Risk Management, Compliance. The unit develops detailed risk profiles, coordinates with external intelligence sources, and prepares comprehensive reports for senior management and regulators. Example: When a multinational corporation seeks a large credit facility, the EDDU reviews the company's ownership structure, scrutinizes recent large cash flows, and validates the legitimacy of the underlying business contracts. Practical application: The EDDU integrates advanced analytics to flag unusual patterns, conducts site visits when necessary, and maintains a repository of high-risk client dossiers. Challenges: Balancing thoroughness with operational efficiency, managing data privacy concerns, and staying current with evolving regulatory expectations.

Financial Action Task Force (FATF) – An intergovernmental body that sets international standards for combating money laundering and terrorist financing. Related: AML, Recommendations, Mutual Evaluations. FATF issues 40 Recommendations that form the global benchmark for national AML/CFT regimes.

Financial Institution (FI) – Any entity that conducts banking, securities, insurance, or other financial services and is therefore subject to AML/CFT obligations. Related: Bank, Broker-Dealer, Insurance Company. FIs must implement risk-based controls, conduct CDD, and report suspicious activity.

Foreign Politically Exposed Person (Foreign PEP) – An individual who holds or has held a prominent public function in a foreign country, along with their immediate family and known associates. Related: PEP, Sanctions, High-Risk Customer. Foreign PEPs are subject to heightened scrutiny due to the potential for corruption and abuse of public office.

Geographic Risk – The level of money-laundering risk associated with a particular country or region, based on factors such as corruption levels, regulatory quality, and prevalence of illicit financial activity. Related: Jurisdictional Risk, Country Risk Rating. Institutions often use FATF's high-risk and non-cooperative jurisdiction lists to calibrate geographic risk scores.

High-Risk Customer – A client whose profile, activity, or jurisdiction places them in a category that warrants additional monitoring and controls. Related: PEP, EDD, Risk Rating. High-risk customers may trigger enhanced monitoring, transaction limits, and periodic senior-management reviews.

Identity Verification – The process of confirming that a customer's claimed identity matches official records, typically through government-issued documents, biometric checks, or third-party databases. Related: KYC, CDD, Authentication. Effective verification reduces the likelihood of synthetic identity fraud.

International Sanctions – Measures imposed by governments or multilateral bodies that restrict financial dealings with designated individuals, entities, or countries. Related: OFAC, UN Sanctions, Blocking Orders. Institutions must screen clients against sanctions lists to avoid prohibited transactions.

Know Your Customer (KYC) – The set of procedures used to collect and verify client identification information at onboarding and during the relationship lifecycle. Related: CDD, AML, Customer Identification Program. KYC is a foundational element of AML compliance and supports risk-based decision making.

Liquidity Risk – The risk that an institution cannot meet its short-term financial obligations due to insufficient cash or liquid assets. Related: Funding Risk, Market Risk. While not directly an AML term, liquidity pressures can incentivize illicit behavior such as rapid cash-out of illicit proceeds.

Money Laundering – The process of disguising the origins of illegally obtained funds to make them appear legitimate. Related: Terrorist Financing, Structuring, Placement. Money laundering typically follows three stages: placement, layering, and integration.

Negative News Screening – The practice of scanning public media and databases for adverse information about a client, such as involvement in corruption, fraud, or other illicit activities. Related: Media Monitoring, Risk Alerts. Negative news can trigger a review or escalation to the EDDU.

Operational Risk – The risk of loss resulting from inadequate or failed internal processes, people, systems, or external events. Related: Compliance Risk, Process Failure. In AML, operational risk includes failures in transaction monitoring, data capture, or reporting.

Politically Exposed Person (PEP) – An individual who holds or has held a prominent public function domestically, along with close family members and associates. Related: Foreign PEP, Corruption Risk, EDD. PEPs are scrutinized because they may exploit their position for personal gain.

Risk Assessment – The systematic evaluation of potential AML/CFT risks associated with customers, products, services, and geographies. Related: Risk Rating, Risk Matrix, Control Framework. Results inform the level of due diligence required and the intensity of ongoing monitoring.

Risk-Based Approach (RBA) – A methodology that tailors AML controls to the specific risk profile of each client and transaction, rather than applying a one-size-fits-all model. Related: Risk Assessment, CDD, EDD. RBA enables efficient allocation of resources toward higher-risk areas.

Sanctions Screening – The automated process of comparing client names and transaction details against government and international sanctions lists. Related: OFAC, UN List, Blocked Party. Failure to screen can result in severe regulatory penalties.

Source-of-Funds (SOF) Analysis – The investigation of where a client's money originates, including the nature of the underlying business, income, or assets. Related: SOE, Wealth Verification, EDD. SOF analysis is a core component of EDD, especially for large or unusual deposits.

Source-of-Wealth (SOW) Analysis – A broader examination of the client's overall wealth accumulation over time, as opposed to a single transaction's origin. Related: SOF, Wealth Screening, Financial Profile. SOW helps detect inconsistencies between declared wealth and observed financial behavior.

Transaction Monitoring – The continuous review of client transactions using rules, thresholds, and analytics to detect suspicious patterns. Related: Alert Generation, SAR, Real-Time Monitoring. Effective monitoring is essential for early detection of money-laundering activities.

Transaction Structuring (Smurfing) – The practice of breaking up large transactions into smaller amounts to avoid detection thresholds. Related: Placement, Threshold Evasion, Alert. Structured transactions often generate alerts that require investigation.

Unusual Activity Report (UAR) – An internal report documenting atypical or suspicious behavior that may not meet formal SAR criteria but warrants further review. Related: SAR, Internal Alert, Risk Review. UARs help maintain a comprehensive audit trail of investigative actions.

Unusual Transaction Monitoring – The application of advanced analytics to identify patterns that deviate from a client's normal behavior, even if each individual transaction falls below reporting thresholds. Related: Behavioral Analytics, Risk Scoring. This approach reduces false negatives for complex laundering schemes.

U.S. Office of Foreign Assets Control (OFAC) – The U.S. Treasury bureau that administers and enforces economic and trade sanctions. Related: Sanctions Screening, SDN List, Blocking. OFAC compliance is mandatory for any entity dealing with U.S. dollars or U.S. persons.

Virtual Asset Service Provider (VASP) – A business that facilitates the exchange, transfer, or custody of virtual currencies, such as cryptocurrencies. Related: AML, CDD, FATF Guidance. VASPs are subject to AML obligations, including KYC and transaction monitoring.

Watch List – A curated collection of individuals, entities, or countries flagged for heightened scrutiny due to suspected involvement in illicit activity. Related: Sanctions List, PEP List, Negative Media. Institutions update watch lists regularly to reflect evolving risks.

World Bank Governance Indicators – A set of metrics that assess the quality of governance in countries, including control of corruption and rule of law. Related: Geographic Risk, Country Rating, FATF. These indicators help shape geographic risk scores for AML purposes.

Anti-Bribery and Corruption (ABC) Program – A set of policies and procedures aimed at preventing bribery and corrupt practices within an organization. Related: AML, Compliance, PEP. ABC programs often intersect with AML controls when dealing with foreign officials.

Automated Risk Scoring – The use of algorithms to assign risk scores to customers based on a combination of static data (e.g., jurisdiction) and dynamic data (e.g., transaction behavior). Related: Risk Rating, Machine Learning, Alert Prioritization. Automated scoring enables the EDDU to prioritize cases efficiently.

Beneficial Ownership Registry – A public or private database that records the ultimate owners of legal entities. Related: Transparency Register, UBO, Corporate Disclosure. Access to such registries assists in verifying ownership structures during EDD.

Compliance Risk – The risk of legal or regulatory sanctions, financial loss, or reputational damage arising from inadequate compliance controls. Related: Operational Risk, AML, Governance. Managing compliance risk involves regular audits, policy updates, and staff training.

Counter-Terrorist Financing (CTF) – Measures aimed at detecting, preventing, and disrupting the flow of funds used to support terrorist activities. Related: AML, SAR, Sanctions. CTF requirements often overlap with AML obligations, especially in transaction monitoring.

Data Privacy Regulations – Laws governing the collection, storage, and processing of personal data, such as GDPR or CCPA. Related: KYC, Data Retention, Confidentiality. Balancing AML data collection with privacy rights is a common challenge for compliance teams.

Dynamic Customer Profiling – The continuous updating of a client’s risk profile based on new information, transaction patterns, and external alerts. Related: Risk Rating, Transaction Monitoring, EDD. Dynamic profiling helps the EDDU detect emerging risks promptly.

Electronic Funds Transfer (EFT) – The movement of money electronically between banks or financial institutions. Related: SWIFT, ACH, Transaction Monitoring. EFTs are subject to AML scrutiny, especially when crossing high-risk borders.

Financial Crime Risk Assessment (FCRA) – A comprehensive evaluation of an institution’s exposure to various financial crime threats, including money laundering, fraud, and corruption. Related: AML Risk Assessment, Control Framework. The FCRA informs the design of controls and the allocation of resources.

General Anti-Money Laundering (GAML) Guidance – Broad regulatory guidance that outlines best practices for AML programs, often issued by supervisory bodies. Related: FATF Recommendations, Regulatory Guidance. GAML helps institutions align with international standards.

High-Value Transaction (HVT) – A transaction that exceeds a predefined monetary threshold, typically triggering enhanced scrutiny. Related: Threshold, SAR, EDD. HVTs are often monitored for structuring or rapid movement of illicit funds.

International Criminal Police Organization (INTERPOL) – A global police agency that facilitates cooperation among law-enforcement authorities. Related: Sanctions, Alerts, Criminal Intelligence. INTERPOL notices can be incorporated into watch lists for AML screening.

Joint Commission on International Banking (JCIB) – An industry consortium that publishes standards for international banking compliance. Related: AML Standards, Best Practices. Membership may provide access to shared resources and benchmarking tools.

Know-Your-Business (KYB) – The process of verifying the legitimacy, ownership, and operational details of a corporate client. Related: CDD, Beneficial Owner, Corporate Disclosure. KYB is critical for onboarding corporate customers and for ongoing monitoring.

Legal Entity Identifier (LEI) – A unique 20-character alphanumeric code assigned to legal entities participating in financial markets. Related: Transparency, Corporate Identification, FATF. LEIs assist in tracing ownership across complex corporate structures.

Liquidity Management – The strategies employed by a financial institution to ensure sufficient cash flow to meet obligations. Related: Operational Risk, Funding Risk. While primarily a treasury function, liquidity constraints can affect AML monitoring capacity.

Money-Laundering Reporting Officer (MLRO) – The senior individual responsible for overseeing AML compliance, receiving SARs, and liaising with regulators. Related: Compliance Officer, EDDU, SAR. The MLRO must ensure that all suspicious activity is reported in a timely manner.

Negative Media Screening – The systematic search of news outlets, blogs, and social media for adverse information about a client. Related: Watch List, Risk Alerts, EDD. Negative media can prompt a deeper investigation by the EDDU.

Operational AML Controls – The day-to-day procedures, such as transaction monitoring rules, customer onboarding checklists, and staff training, that operationalize the AML program. Related: Control Framework, Risk Management. Effective controls reduce the likelihood of missed alerts.

Payment Card Industry Data Security Standard (PCI DSS) – A set of security standards for organizations that handle credit-card information. Related: Data Privacy, Compliance, Cybersecurity. While not an AML standard, PCI DSS compliance can intersect with AML when analyzing payment-card transaction patterns.

Political Risk – The risk that a client’s operations may be affected by changes in political conditions, such as regime change or policy shifts. Related: PEP, Sanctions, Geographic Risk. Political risk assessments help determine the need for EDD.

Real-Time Monitoring – The capability to evaluate transactions as they occur, enabling immediate detection of suspicious activity. Related: Transaction Monitoring, Alert Generation. Real-time monitoring is increasingly supported by AI-driven engines.

Regulatory Examination – An on-site or off-site review conducted by supervisory authorities to assess an institution's compliance with AML regulations. Related: Audit, Supervisory Review, Findings. Findings from examinations often lead to remediation actions for the EDDU.

Risk Appetite – The level of risk an organization is willing to accept in pursuit of its objectives. Related: Risk Tolerance, Governance, AML Strategy. Defining risk appetite guides the intensity of due-diligence procedures.

Risk Governance – The framework of policies, committees, and oversight mechanisms that direct risk management activities. Related: Board, Compliance Committee, Risk Culture. Strong risk governance ensures that AML risks are addressed at the appropriate seniority level.

Risk Matrix – A visual tool that plots risk likelihood against impact to prioritize remediation efforts. Related: Risk Assessment, Heat Map, Control Prioritization. The EDDU may use a risk matrix to allocate investigative resources.

Risk Rating – A numeric or categorical score assigned to a client based on its assessed risk level. Related: Risk Assessment, Automated Scoring, Tiering. Clients with high risk ratings typically undergo EDD.

Sanctions List – An official compilation of individuals, entities, and regimes subject to trade or financial restrictions. Related: OFAC, UN List, Blocking. Regular updates to sanctions lists are essential for accurate screening.

Screening Tool – Software that automates the comparison of client data against watch lists, sanctions, and PEP databases. Related: AML Software, Alert Generation. Effective tools reduce manual effort and improve detection rates.

Sector-Specific Risk – The inherent AML risk associated with particular industries, such as casinos, real estate, or precious metals. Related: High-Risk Industry, EDD, Risk Weighting. Institutions may apply higher risk weights to customers operating in these sectors.

Senior Management Oversight – The responsibility of executives and the board to ensure that AML policies are adequately designed, implemented, and resourced. Related: Governance, Risk Appetite, Compliance. Senior oversight is required by most AML regulations.

Source-of-Funds Verification – The process of obtaining documentary evidence (e.g., tax returns, sale contracts) to substantiate the origin of a specific sum of money. Related: SOF Analysis, EDD, Documentation. Verification is a key step when large deposits are made into a new account.

Transaction Alert – A notification generated by monitoring systems indicating that a transaction matches predefined suspicious criteria. Related: SAR, Alert Management, EDDU. Alerts are investigated by analysts and may be escalated to the EDDU for deeper review.

Transaction Monitoring Rules – The set of logical conditions (e.g., thresholds, frequency, counterparties) that define what constitutes a potentially suspicious transaction. Related: Rule Engine, Alert Generation. Rules are calibrated based on risk assessments and can be tuned over time.

Transaction Profile – The historical pattern of a client’s transaction behavior, including typical amounts, frequencies, and counterparties. Related: Behavioral Analytics, Baseline, Dynamic Profiling. Deviations from the profile often trigger alerts.

Unstructured Data Analysis – The examination of non-tabular information such as emails, PDFs, and social-media posts for AML insights. Related: AI, Text Mining, Risk Indicators. Unstructured data can reveal hidden connections between entities.

Virtual Currency Exchange (VCE) – A platform that allows users to convert fiat currency into virtual assets and vice versa. Related: VASP, AML, CDD. VCEs must implement robust KYC and transaction monitoring to prevent illicit use.

Watch-List Consolidation – The process of merging multiple sanction, PEP, and adverse-media lists into a single, deduplicated database for efficient screening. Related: Data Hygiene, Screening Tool. Consolidation improves performance and reduces false positives.

Whistleblower Program – An internal mechanism that encourages employees to report suspected misconduct, including AML violations, without fear of retaliation. Related: Compliance Culture, Reporting, Investigation. Effective programs can surface hidden risks that automated systems miss.

World Economic Forum (WEF) Global Risks Report – An annual publication that identifies and assesses major global risks, including financial crime trends. Related: Risk Landscape, Emerging Threats. Institutions may reference the report when updating risk assessments.

Zero-Tolerance Policy – An organizational stance that any breach of AML rules will be met with strict disciplinary action. Related: Compliance Culture, Enforcement, Sanctions. While aspirational, such policies reinforce the seriousness of AML obligations.