Graduate Certificate in Know Your Customer and Anti-Money Laundering Compliance

Customer Due Diligence

Adverse Media – related terms: negative news, reputational risk. Information from newspapers, online sources, or broadcast media that indicates a potential client may be involved in illicit activity. Example: a news article linking a business owner to fraud triggers a deeper review. Practical application includes integrating media monitoring tools into the CDD workflow. Challenges involve distinguishing rumor from verified facts and managing the volume of data.

Beneficial Owner – related terms: ultimate owner, equity interest. The natural person who ultimately owns or controls a customer, directly or indirectly. For a shell company, the beneficial owner may be hidden behind layers of ownership. In practice, analysts must trace ownership structures using registries and shareholder lists. The main challenge is dealing with jurisdictions that do not publicly disclose ownership information.

Customer Due Diligence (CDD) – related terms: KYC, risk assessment. The process of collecting and verifying information about a customer to assess money-laundering risk. It includes identity verification, understanding the nature of the business, and ongoing monitoring. For a new corporate client, CDD may involve reviewing incorporation documents and board minutes. Challenges include balancing thoroughness with customer experience and keeping records up to date.

Enhanced Due Diligence (EDD) – related terms: high-risk client, deeper investigation. A more intensive form of CDD applied when a customer presents a higher risk of money-laundering or terrorist financing. Example: a PEP from a high-risk jurisdiction requires verification of source of wealth, additional senior-management approvals, and periodic reviews. The difficulty lies in obtaining reliable source-of-funds documentation and managing the increased workload.

Financial Action Task Force (FATF) – related terms: international standards, AML/CTF. An inter-governmental body that sets global AML and counter-terrorist financing (CTF) standards. FATF recommendations drive national legislation and influence the design of CDD programs. Practically, compliance officers reference FATF guidance when drafting policies. A challenge is keeping pace with FATF updates and translating them into local procedures.

Foreign Politically Exposed Person (Foreign PEP) – related terms: domestic PEP, senior political figure. An individual who holds or has held a prominent public function in a foreign country, or a close associate or family member of such an individual. Example: the spouse of a foreign head of state opening a bank account triggers EDD. Practitioners must verify the PEP's relationship, source of wealth, and monitor transactions for unusual activity. The main challenge is the cross-border nature of information sharing and differing definitions across jurisdictions.

Financial Institution – related terms: regulated entity, banking sector. Any entity that conducts financial services, such as banks, credit unions, insurers, and investment firms, and is subject to AML/CTF regulations. CDD obligations apply to all customers of financial institutions. In practice, a bank must apply CDD to retail,

corporate, and correspondent banking relationships. Challenges include coordinating CDD across multiple business lines and legacy systems.

Identification Documents – related terms: primary ID, secondary ID. Official documents used to verify a customer's identity, such as passports, driver's licences, and national ID cards. For a non-resident individual, a passport combined with a utility bill may satisfy verification requirements. Practical considerations include document authenticity checks, handling expired documents, and complying with data-privacy laws. The challenge is balancing thorough verification with the risk of forging or tampering.

In-Person Verification – related terms: face-to-face, electronic verification. The act of confirming a customer's identity through a physical meeting, often required for high-risk or high-value accounts. Example: a private banking client meeting a compliance officer to present original documents. This method reduces reliance on electronic data but can be costly and time-consuming, especially for remote clients.

International Sanctions List – related terms: OFAC, UN sanctions, embargoes. Lists compiled by governments or international bodies that identify individuals, entities, or countries subject to trade or financial restrictions. Screening a new client against the OFAC SDN list is a standard CDD step. Practical application includes automated screening tools that flag matches for analyst review. Challenges arise from false positives, name variations, and updating lists in real time.

Key Risk Indicators (KRIs) – related terms: metrics, monitoring thresholds. Quantifiable measures used to identify potential AML/CTF risks within a CDD program. Examples include sudden spikes in transaction volume, high-risk jurisdiction exposure, or rapid changes in ownership. KRIs help prioritize investigative resources. The difficulty lies in selecting meaningful indicators that avoid alert fatigue.

KYC (Know Your Customer) – related terms: CDD, client onboarding. The collective set of processes used to collect, verify, and maintain accurate information about a customer. KYC is the foundation upon which CDD and EDD are built. In practice, a fintech platform may use digital identity verification to satisfy KYC requirements. Challenges include adapting KYC to emerging technologies such as blockchain and ensuring consistent application across channels.

Legal Entity Identifier (LEI) – related terms: global identifier, GLEIF. A 20-character alphanumeric code that uniquely identifies a legal entity participating in financial transactions. An LEI simplifies the process of locating beneficial owners and assessing risk. For a multinational corporation, the LEI can be used to aggregate exposure across subsidiaries. The challenge is ensuring the LEI data remains current and matches the client's official registration.

Money Laundering – related terms: placement, layering, integration. The process of disguising the origins of illegally obtained funds to make them appear legitimate. CDD seeks to prevent the placement stage by verifying the source of funds. Practical examples include monitoring cash-intensive businesses for structuring attempts. The challenge is that sophisticated laundering schemes can evade detection without robust CDD.

Negative News Screening – related terms: adverse media, reputational risk. The practice of searching public sources for information that may indicate illicit behavior by a customer. Screening is performed at

onboarding and periodically thereafter. An example is an automated tool flagging a client whose name appears in a fraud investigation report. Challenges involve language barriers, differing legal standards for defamation, and managing false alerts.

Non-Resident Customer – related terms: offshore client, cross-border. An individual or entity that does not reside in the jurisdiction where the financial institution operates. CDD for non-resident customers often requires additional documentation, such as proof of address and source of wealth. Practical application includes requiring a notarised declaration of residency. The main challenge is the higher inherent risk due to limited local oversight.

Off-Shore Jurisdiction – related terms: tax haven, secrecy jurisdiction. A country or territory that offers financial services to non-resident clients with favorable tax or regulatory regimes. CDD in offshore contexts demands rigorous verification of ownership structures and source of funds. Example: a trust established in a known secrecy jurisdiction requires EDD. Challenges include limited public registers and heightened scrutiny from regulators.

Operational Risk – related terms: process failure, compliance breach. The risk of loss resulting from inadequate or failed internal processes, people, or systems. In CDD, operational risk may manifest as missed alerts, data entry errors, or insufficient training. Mitigation involves robust SOPs, regular audits, and staff competency assessments. The difficulty lies in quantifying risk and aligning it with AML objectives.

PEP (Politically Exposed Person) – related terms: senior public official, family member. An individual who holds or has held a prominent public function, along with close associates and family. Domestic PEPs include ministers, judges, and senior military officers. CDD for PEPs typically involves EDD, senior-management approval, and ongoing monitoring. The challenge is the subjectivity in determining “close association” and the dynamic nature of political appointments.

Risk Assessment – related terms: risk matrix, threat profile. The systematic process of identifying, evaluating, and prioritizing AML/CTF risks associated with customers, products, services, and geographies. An institution may assign a risk rating (low, medium, high) based on factors such as transaction volume and jurisdiction. Practical use includes tailoring CDD intensity accordingly. Challenges include data quality, subjectivity in scoring, and ensuring regular updates.

Sanctions Compliance – related terms: embargo, watchlist. The set of policies and procedures designed to ensure that a financial institution does not engage with sanctioned persons or entities. It incorporates screening, transaction blocking, and reporting obligations. Example: a bank must freeze assets of a customer flagged on the UN sanctions list. The main challenge is reconciling conflicting sanctions regimes and handling high-volume screening efficiently.

Source of Funds (SOF) – related terms: source of wealth, financial origin. The specific money used to fund a particular transaction or account. Verification may involve bank statements, invoices, or contracts. For a large cash deposit, the institution must request a detailed explanation and supporting documents. The challenge is obtaining credible SOF evidence, especially when customers deal in cash-intensive businesses.

Source of Wealth (SOW) – related terms: net worth, asset accumulation. The overall origin of a customer’s

total assets, not just the money used in a single transaction. SOW analysis becomes critical for high-net-worth individuals. Example: a client's wealth derived from a family-owned manufacturing business requires review of financial statements and tax returns. Challenges include privacy concerns and the depth of documentation required.

Suspicious Activity Report (SAR) – related terms: suspicious transaction, regulator filing. A report filed by a financial institution to the relevant authority when a transaction or behavior appears suspicious. CDD failures often lead to SAR filings. For instance, a series of rapid transfers to a high-risk jurisdiction may trigger a SAR. The reporting process must protect confidentiality, and the challenge is ensuring accurate, timely filing without over-reporting.

Transaction Monitoring – related terms: real-time alerts, rule-based engine. The systematic review of customer transactions to detect patterns indicative of money laundering or terrorist financing. Monitoring rules may flag structuring, rapid movement of funds, or activity inconsistent with a customer's profile. Practical application includes configuring thresholds in the monitoring system based on risk ratings. Challenges involve balancing sensitivity to catch illicit activity while minimizing false positives.

Ultimate Beneficial Owner (UBO) – related terms: beneficial owner, ownership chain. The natural person who ultimately controls a legal entity, even if ownership is layered through intermediaries. Identifying the UBO is essential for effective CDD. Example: a holding company owned by another corporation, which in turn is owned by an individual, requires tracing through multiple registries. The difficulty lies in jurisdictions that do not require disclosure of UBO information.

Virtual Asset Service Provider (VASP) – related terms: crypto exchange, digital wallet. An entity that conducts activities involving virtual assets, such as exchange, custody, or transfer services. AML regulations now require VASPs to implement CDD similar to traditional financial institutions. Practical steps include verifying wallet ownership and monitoring blockchain transactions. Challenges include the pseudonymous nature of blockchain and rapidly evolving regulatory guidance.

Watchlist Screening – related terms: sanctions list, PEP database. The process of comparing customer data against various watchlists to identify matches. Screening is performed at onboarding and on an ongoing basis. Example: a customer's name matches an entry on the EU consolidated sanctions list, prompting a manual review. The main challenge is handling name variations, transliterations, and ensuring timely updates.

Wire Transfer Monitoring – related terms: SWIFT, cross-border payments. The surveillance of electronic funds transfers for suspicious patterns. Institutions may apply rule-sets that flag transfers exceeding certain amounts to high-risk jurisdictions. Practical use includes automatic alerts for transfers that deviate from a customer's typical behavior. Challenges involve high transaction volumes, data quality, and differentiating legitimate business payments from illicit flows.

Anti-Money Laundering (AML) – related terms: CDD, compliance program. The collective set of laws, regulations, and procedures designed to prevent the generation of illicit funds. CDD is a core component of an AML framework. Example: a bank implements an AML policy that mandates EDD for customers from high-risk countries. The challenge is integrating AML controls across diverse business units while

maintaining operational efficiency.

Anti-Terrorist Financing (CTF) – related terms: AML, sanctions. Measures aimed at preventing the provision of funds to support terrorist activities. CDD helps identify potential terrorist financiers by assessing source of funds and links to known terror groups. Practical application includes screening against terrorist watchlists. Challenges include the dynamic nature of terrorist networks and the need for rapid intelligence sharing.

Automated Decision-Making (ADM) – related terms: AI, machine learning. The use of algorithms to assess risk and make CDD decisions without human intervention. For example, an AI model may assign a risk score based on data points such as jurisdiction, transaction patterns, and public records. Benefits include speed and consistency; however, challenges include model bias, lack of transparency, and regulatory acceptance.

Beneficial Ownership Register – related terms: public register, corporate transparency. A database where companies disclose their UBOs, often mandated by law. CDD officers consult the register to verify ownership information. Example: a UK company's filing shows a private individual as the sole UBO. Challenges arise when registers are incomplete, outdated, or unavailable for offshore entities.

Conduct Risk – related terms: ethical standards, compliance culture. The risk that a financial institution's behavior may lead to regulatory or reputational damage. Weak CDD processes can increase conduct risk by exposing the firm to illicit activity. Mitigation includes training, tone-from-the-top, and robust monitoring. The difficulty is measuring conduct risk quantitatively.

Corporate Governance – related terms: board oversight, internal controls. The system of rules, practices, and processes by which a company is directed and controlled. Effective governance supports accurate CDD by ensuring proper sign-off on high-risk clients. Example: a board committee reviews all EDD cases exceeding a predefined threshold. Challenges include aligning governance structures with AML expectations across subsidiaries.

Data Privacy – related terms: GDPR, confidentiality. Legal frameworks that protect personal information collected during CDD. Institutions must balance AML obligations with privacy rights, such as limiting data retention to the necessary period. Practical steps include anonymising non-essential data and obtaining explicit consent where required. Challenges emerge when privacy laws conflict with AML reporting duties.

Denial-of-Service (DoS) Attack – related terms: cyber risk, system availability. While not a direct CDD concept, DoS attacks can disrupt AML systems, affecting real-time screening and monitoring. Institutions must ensure business continuity plans cover AML technology. The challenge is allocating resources to protect systems that are not traditionally deemed "customer-facing".

Digital Identity Verification – related terms: e-KYC, biometric authentication. The use of electronic methods to confirm a customer's identity, often through facial recognition, document scanning, and liveness checks. Example: a mobile-banking app requests a selfie and passport scan to complete onboarding. Benefits include speed and remote accessibility; challenges involve fraud detection, data security, and regulatory acceptance of digital proofs.

Economic Sanctions – related terms: trade embargo, export control. Restrictions imposed by governments to prohibit certain economic activities with designated persons or countries. CDD must identify any exposure to sanctioned parties before establishing a relationship. Practical application includes real-time sanctions screening of new accounts. The difficulty lies in interpreting complex sanction regimes and handling overlapping restrictions.

Electronic Funds Transfer (EFT) – related terms: ACH, SEPA. A transfer of money conducted electronically between banks. CDD processes must assess the legitimacy of EFTs, especially when they involve high-risk jurisdictions. Example: a sudden EFT to a shell company in a tax haven may trigger enhanced monitoring. Challenges include high transaction volumes and limited visibility into the ultimate beneficiary.

Enterprise Risk Management (ERM) – related terms: risk appetite, governance. A holistic approach to identifying and managing all significant risks across an organization, including AML/CTF risks. CDD is integrated into ERM through risk-based policies and reporting structures. Practical use includes aligning AML risk appetite with overall corporate risk thresholds. The challenge is ensuring AML risk is not siloed but considered in strategic decisions.

Financial Crime – related terms: fraud, money laundering. A broad term encompassing illegal activities that involve the misuse of financial systems. CDD is a frontline defense against financial crime. Example: a client engaged in fraudulent insurance claims may be identified through unusual claim patterns. Challenges include the evolving nature of crime tactics and the need for cross-functional collaboration.

FinCEN (Financial Crimes Enforcement Network) – related terms: US regulator, SAR filing. The US Treasury bureau that enforces AML laws and collects SARs. Institutions operating in the United States must comply with FinCEN regulations, including CDD requirements for foreign correspondent accounts. Practical implications involve filing SARs within prescribed timeframes. The challenge is staying current with FinCEN updates and interpreting guidance for complex structures.

Geographic Risk – related terms: jurisdictional risk, high-risk country. The assessment of AML risk based on the location of a customer, its operations, or transaction destinations. A client operating in a country with weak AML controls receives a higher risk rating. Practical application includes using FATF country ratings to inform CDD intensity. Challenges include managing customers with multi-jurisdictional exposure and updating risk matrices as country risk profiles evolve.

High-Risk Customer – related terms: PEP, offshore entity. A client that presents a higher likelihood of involvement in money laundering due to factors such as political exposure, complex ownership, or activity in sanctioned jurisdictions. High-risk customers require EDD, senior-management approval, and more frequent reviews. The challenge is correctly identifying high-risk characteristics without over-burdening low-risk clients.

Identity Verification Service (IVS) – related terms: third-party provider, KYC API. A service that validates identity documents against authoritative databases. Financial institutions may integrate an IVS to automate the KYC step. Example: an IVS checks a passport number against a government registry. Benefits include speed and reduced manual effort; challenges involve data security, vendor reliability, and regulatory acceptance of third-party verification.

International Financial Reporting Standards (IFRS) – related terms: accounting standards, financial statements. Global accounting standards that influence the financial reporting of corporate clients. While not a direct CDD element, understanding IFRS statements aids analysts in assessing a client's financial health and source of wealth. The challenge is interpreting complex disclosures and reconciling them with AML risk assessments.

Joint Account – related terms: co-ownership, shared liability. An account held by two or more individuals, each having rights to the funds. CDD must verify each account holder's identity and assess combined risk. Example: a married couple jointly owning a high-value investment account may trigger combined source-of-wealth analysis. Challenges include managing differing risk profiles and ensuring all parties are adequately screened.

KYC Refresh – related terms: periodic review, data update. The process of updating a customer's information at regular intervals to ensure continued compliance. Typically, high-risk clients are reviewed annually, while low-risk clients may be refreshed every three years. Practical steps include sending secure questionnaires and re-verifying documents. The challenge is maintaining timely updates without causing client fatigue.

Liquidity Risk – related terms: cash flow, funding stability. While primarily a banking risk, liquidity concerns can intersect with AML when large, unexplained cash movements occur. CDD analysts monitor for sudden liquidity injections that lack a clear business rationale. Example: a sudden influx of cash into a low-volume account may indicate structuring. Challenges involve distinguishing legitimate cash flow spikes from illicit activity.

Money Laundering Reporting Officer (MLRO) – related terms: compliance head, SAR authority. The senior individual responsible for overseeing the AML program, including CDD policies and SAR filings. The MLRO ensures that CDD procedures are properly implemented and that suspicious activity is escalated appropriately. Practical duties include conducting risk assessments and reporting to senior management. Challenges include balancing independence with organizational pressures.

Negative Control List – related terms: prohibited entities, compliance blacklist. A list of individuals or organisations that a financial institution is expressly prohibited from dealing with, often derived from sanctions, anti-terrorism, or internal policy. Screening against the negative control list is a mandatory CDD step. Challenges include maintaining an up-to-date list and handling inadvertent matches.

Off-Balance-Sheet Exposure – related terms: contingent liability, credit risk. Financial obligations not recorded on the balance sheet but that may pose AML risk, such as guarantees or letters of credit. CDD must consider these exposures when evaluating a client's overall risk. Example: a corporation obtains a standby letter of credit for a high-risk transaction, prompting additional scrutiny. The challenge is obtaining visibility into these hidden commitments.

Operational Due Diligence (ODD) – related terms: vendor risk, third-party assessment. The review of a service provider's processes, controls, and compliance posture. When outsourcing CDD functions to a third-party vendor, ODD ensures that the provider meets regulatory standards. Practical steps include reviewing the vendor's AML policies and audit reports. Challenges involve managing data protection obligations and ensuring consistent standards across providers.

Political Risk – related terms: regime change, expropriation. The risk that political events will affect a client's operations or the legitimacy of funds. CDD analysts assess political risk when evaluating clients operating in unstable regions. Example: a mining company in a country experiencing civil unrest may be subject to heightened monitoring. Challenges include forecasting political developments and quantifying their impact on AML risk.

Regulatory Reporting – related terms: SAR, CTR. The mandatory submission of information to supervisory authorities, such as suspicious activity reports or currency transaction reports. Accurate CDD data underpins the quality of regulatory reporting. Practical considerations include meeting filing deadlines and preserving confidentiality. The challenge is ensuring data integrity across multiple reporting systems.

Risk Appetite – related terms: tolerance level, board decision. The amount and type of risk an organization is willing to accept in pursuit of its objectives. AML risk appetite influences how aggressively CDD procedures are applied. For example, a low risk-appetite may mandate EDD for all corporate clients. Challenges include aligning risk appetite with business growth goals and communicating it effectively throughout the firm.

Sanctions Evasion – related terms: circumvention, indirect dealing. The act of conducting prohibited transactions through intermediaries or complex structures to avoid detection. CDD must uncover layers that mask the true beneficiary of a transaction. Example: a shell company in a non-sanctioned country is used to route funds to a sanctioned individual. Challenges include limited transparency in certain jurisdictions and sophisticated structuring techniques.

Sector-Specific Risk – related terms: industry typology, high-risk sector. The assessment of AML risk based on the nature of the client's business. Certain sectors, such as casinos, real estate, and precious metals, are considered higher risk. CDD policies may require additional documentation for these sectors. The challenge is maintaining an up-to-date sector risk matrix as new business models emerge.

Shareholder Register – related terms: equity ledger, ownership record. A record of individuals or entities that hold shares in a company. Reviewing the register helps identify UBOs during CDD. Practical use includes cross-checking the register against public filings. Challenges arise when shareholders use nominee arrangements that conceal true ownership.

Structured Transaction – related terms: layering, smurfing. A series of related financial movements designed to obscure the origin of funds. CDD may detect structured transactions through monitoring for multiple small deposits below reporting thresholds. Example: a client makes a series of cash deposits just under the $10,000 reporting limit. The challenge is distinguishing legitimate business practices from deliberate structuring.

Third-Party Risk – related terms: outsourcing, vendor due diligence. The risk that a service provider's failure to comply with AML standards can expose the institution to regulatory penalties. When delegating CDD to a third-party, ODD must be performed. Practical steps include contractual clauses requiring adherence to AML regulations. Challenges include ensuring consistent oversight and handling cross-border data transfers.

Transaction Threshold – related terms: reporting limit, alert trigger. A predefined monetary amount that,

when exceeded, initiates additional CDD steps or monitoring. For example, a $50,000 cash deposit may automatically generate a senior-management review. The challenge is setting thresholds that are high enough to avoid excessive alerts but low enough to capture suspicious activity.

True Beneficial Owner (TBO) – related terms: ultimate owner, control person. The individual who ultimately enjoys the benefits of ownership, even if not formally listed as a shareholder. Identifying the TBO is critical for high-risk entities. Example: a trust where the settlor, protector, and beneficiary are all the same individual. Challenges include opaque trust structures and limited disclosure requirements.

Unusual Activity – related terms: red flag, anomaly. Any transaction or behavior that deviates from a customer's normal pattern or appears inconsistent with the stated business purpose. CDD staff must investigate such activity, potentially escalating to a SAR. Example: a low-risk retail client suddenly transfers large sums to a high-risk jurisdiction. The challenge is defining "unusual" in a way that captures genuine risk without overwhelming staff.

Virtual Asset – related terms: cryptocurrency, digital token. A digitised representation of value that can be transferred electronically. VASPs must apply CDD when onboarding users who hold or trade virtual assets. Practical steps include verifying wallet ownership and monitoring blockchain transactions for mixing services. Challenges involve the pseudonymous nature of many assets and rapidly evolving regulatory frameworks.

Watchlist Matching – related terms: fuzzy logic, name screening. The technical process of comparing a customer's name and identifiers to entries on a watchlist. Advanced matching algorithms use phonetic and similarity scoring to reduce false negatives. Example: "Johnathan Smith" is matched to "Jon Smith" on a sanctions list. Challenges include handling diacritics, transliteration, and common names that generate high false-positive rates.

Wire Transfer Reporting – related terms: STR, AML filing. The requirement to report certain wire transfers that may be linked to illicit activity, often based on thresholds or suspicious indicators. CDD provides the necessary context to determine whether a wire transfer should be reported. Practical application includes generating a report that details the sender, receiver, purpose, and supporting evidence. Challenges include ensuring timely submission and accurate documentation.

Zero-Risk Assumption – related terms: complacency, risk tolerance. The erroneous belief that a particular client or transaction carries no AML risk, leading to insufficient CDD. Institutions must avoid this mindset by applying risk-based principles. Example: assuming a long-standing client is low-risk without periodic review may miss emerging threats. The challenge is fostering a culture of continuous vigilance.