
Compliance and Anti Money Laundering

Financial Crime Prevention

Anti-Money Laundering (AML) Program – A structured set of policies, procedures, and controls designed to detect, deter, and report money-laundering activities.

Related terms: compliance, risk-based approach, internal controls.

Explanation: An AML program typically includes customer due diligence, transaction monitoring, staff training, and independent testing.

Practical application: A bank implements a layered screening system that flags high-risk customers and automatically generates alerts for further review.

Challenges: Keeping the program up-to-date with evolving regulations and typologies while maintaining operational efficiency.

Beneficial Owner – The natural person who ultimately owns or controls a customer, either directly or indirectly.

Related terms: ultimate beneficial owner (UBO), ownership structure, transparency.

Explanation: Identifying the beneficial owner is essential for assessing the true risk posed by a client, especially when dealing with corporate entities or trusts.

Example: A shell company registered in a tax haven lists a nominee director; the AML officer must trace the underlying individual who benefits from the entity's activities.

Challenges: Complex corporate layers, privacy laws, and resistance from clients can impede accurate identification.

Correspondent Banking – A banking relationship where one bank (the correspondent) provides services on behalf of another bank (the respondent) in a different jurisdiction.

Related terms: cross-border payments, financial institution, due diligence.

Explanation: Correspondent banks facilitate international trade and remittances but are vulnerable to money-laundering because the correspondent may have limited visibility into the respondent's client base.

Practical application: A correspondent bank conducts enhanced due diligence on high-risk respondents, including reviewing their AML controls and transaction patterns.

Challenges: Balancing the need for swift cross-border services with thorough risk assessment, especially when dealing with jurisdictions of varying regulatory standards.

Customer Due Diligence (CDD) – The process of collecting and verifying information about a customer to assess the risk they pose.

Related terms: know your customer (KYC), risk assessment, onboarding.

Explanation: CDD involves verifying identity documents, understanding the purpose of the business relationship, and monitoring for changes over time.

Example: During onboarding, a retail bank obtains a passport, proof of address, and source-of-funds documentation from a new corporate client.

Challenges: High volumes of new customers, data quality issues, and the need to integrate CDD data across multiple systems.

Enhanced Due Diligence (EDD) – Additional scrutiny applied to customers or transactions that present a higher risk of money laundering or terrorist financing.

Related terms: high-risk customers, red flags, senior management approval.

Explanation: EDD may involve deeper background checks, senior-level approvals, and ongoing monitoring of transaction patterns.

Practical application: A financial institution conducts EDD on a politically exposed person (PEP) by reviewing media reports, ownership structures, and transaction histories.

Challenges: Resource intensity, potential delays in customer onboarding, and the difficulty of obtaining reliable information in certain jurisdictions.

Financial Action Task Force (FATF) – An intergovernmental body that sets international standards to combat money laundering, terrorist financing, and related threats.

Related terms: FATF Recommendations, mutual evaluations, high-risk jurisdictions.

Explanation: FATF issues 40 Recommendations that serve as the global benchmark for AML/CTF regimes, and conducts peer reviews of member countries.

Example: A jurisdiction deemed “non-cooperative” by FATF may face increased scrutiny and higher transaction costs from global banks.

Challenges: Keeping national regulations aligned with FATF updates and ensuring effective implementation across diverse legal systems.

Financial Crime Risk Assessment (FCRA) – A systematic process to identify, assess, and prioritize the risks of financial crime that an organization faces.

Related terms: risk matrix, mitigation strategies, governance.

Explanation: FCRA evaluates factors such as customer types, product offerings, geographic exposure, and transaction channels to determine overall risk exposure.

Practical application: A fintech firm uses a risk matrix to assign scores to each client based on jurisdiction, transaction volume, and industry, guiding its monitoring intensity.

Challenges: Dynamic risk landscape, data silos, and the need for regular reassessment as business models evolve.

FATF Recommendations – A set of 40 standards that outline the measures governments and financial institutions should implement to combat money laundering and terrorist financing.

Related terms: AML legislation, compliance frameworks, best practices.

Explanation: The Recommendations cover criminalization, preventive measures, international cooperation, and transparency of beneficial ownership.

Example: Recommendation 10 requires financial institutions to conduct CDD, while Recommendation 16

mandates the filing of suspicious transaction reports.

Challenges: Translating broad recommendations into specific, actionable policies that fit an organization's risk profile.

Know Your Customer (KYC) – The process of verifying the identity of a client and understanding their financial activities to mitigate risk.

Related terms: CDD, onboarding, verification.

Explanation: KYC is the foundational step in AML compliance, requiring collection of identification documents, proof of address, and purpose of the relationship.

Example: An online bank uses biometric verification and document scanning to satisfy KYC requirements for new account openings.

Challenges: Balancing user experience with stringent verification, especially in digital-only channels.

Money Laundering – The process of concealing the origins of illegally obtained funds to make them appear legitimate.

Related terms: placement, layering, integration, typologies.

Explanation: Money laundering typically follows three stages: placement (introducing illicit funds into the financial system), layering (complex transactions to obscure the source), and integration (re-entering the funds into the economy as clean money).

Example: A drug trafficker deposits cash into multiple accounts, uses shell companies to transfer funds internationally, and purchases real estate to legitimize the proceeds.

Challenges: Detecting sophisticated layering schemes, especially when they involve multiple jurisdictions and emerging technologies.

Money Laundering Typologies – Common patterns or methods used by criminals to launder illicit funds.

Related terms: structuring, trade-based schemes, virtual assets.

Explanation: Understanding typologies helps institutions develop targeted controls and alerts. Typical typologies include structuring (smurfing), trade-based money laundering, and the use of cryptocurrency mixers.

Practical application: An AML system incorporates rule sets that trigger alerts when multiple cash deposits just below reporting thresholds occur within a short period.

Challenges: Evolving criminal methods, limited data on new schemes, and the need for continuous analyst training.

Politically Exposed Person (PEP) – An individual who holds a prominent public function, or a close associate or family member of such a person.

Related terms: enhanced due diligence, senior political figure, corruption risk.

Explanation: PEPs pose a higher risk of involvement in corruption and bribery, requiring additional scrutiny and monitoring.

Example: A bank conducts EDD on a senior minister by reviewing the source of wealth, monitoring for large, unusual transactions, and obtaining senior management approval for the relationship.

Challenges: Identifying indirect relationships, managing privacy concerns, and keeping PEP lists current amid frequent political changes.

Sanctions Screening – The process of comparing customers and transactions against lists of individuals, entities, or countries subject to economic sanctions.

Related terms: watch-list, OFAC, UN sanctions, false positives.

Explanation: Screening helps prevent prohibited dealings that could result in legal penalties or reputational damage.

Practical application: A trade finance department uses automated screening software to check every new counterpart against the OFAC Specially Designated Nationals (SDN) list.

Challenges: High volume of alerts, keeping lists up-to-date, and balancing thoroughness with operational efficiency.

Sectoral Risk – The level of money-laundering risk associated with a particular industry or business sector.

Related terms: high-risk sectors, risk weighting, regulatory guidance.

Explanation: Certain sectors, such as casinos, real estate, and precious metals, are considered higher risk due to cash intensity or complex ownership structures.

Example: A bank assigns higher risk scores to clients in the gambling industry, prompting more frequent transaction reviews.

Challenges: Accurately calibrating risk scores and avoiding over- or under-classification.

Suspicious Activity Report (SAR) – A filing made by a financial institution to the relevant authority detailing a suspected instance of money laundering or other illicit activity.

Related terms: filing threshold, confidentiality, regulatory body.

Explanation: SARs are confidential reports that enable law enforcement agencies to investigate potential crimes. Institutions must file SARs promptly when they detect unusual or suspicious behavior.

Example: An AML analyst observes a series of rapid, high-value wire transfers to a high-risk jurisdiction and submits a SAR to the Financial Intelligence Unit.

Challenges: Determining what constitutes sufficient suspicion, managing the volume of SARs, and protecting the reporting entity from retaliation.

Transaction Monitoring – Ongoing analysis of customer transactions to detect patterns that may indicate money laundering or terrorist financing.

Related terms: rule-based alerts, machine learning, threshold.

Explanation: Monitoring systems compare transactional data against predefined rules and risk indicators, generating alerts for analyst review.

Practical application: A bank's monitoring platform flags a sudden increase in inbound transfers from a previously dormant account, prompting a manual investigation.

Challenges: High false-positive rates, integration of new data sources, and adapting rules to emerging threats.

Trade-Based Money Laundering (TBML) – The use of international trade transactions to disguise the origins of illicit funds.

Related terms: over-/under-invoicing, false documentation, commodity fraud.

Explanation: TBML exploits the complexity of trade documentation and the opacity of supply chains to move money across borders.

Example: A exporter inflates invoice amounts for goods shipped to a shell company, allowing the illicit funds to be transferred under the guise of legitimate trade.

Challenges: Detecting TBML requires deep knowledge of trade practices, access to trade data, and sophisticated analytical tools.

Virtual Asset Service Provider (VASP) – A business that conducts activities involving virtual assets, such as cryptocurrency exchanges, wallet providers, and custodians.

Related terms: crypto-exchange, AML for cryptocurrencies, FATF guidance.

Explanation: VASPs are subject to AML/CTF obligations, including KYC, transaction monitoring, and SAR filing.

Practical application: A cryptocurrency exchange implements KYC procedures, monitors blockchain transactions for mixing services, and reports suspicious activity to the relevant authority.

Challenges: Pseudonymous nature of blockchain, rapid innovation, and regulatory uncertainty across jurisdictions.

Whistleblower Protection – Legal and organizational measures that safeguard individuals who report wrongdoing from retaliation.

Related terms: internal reporting, protected disclosure, compliance hotline.

Explanation: Effective whistleblower programs encourage employees to report suspicious activities, enhancing an organization's detection capabilities.

Example: A bank establishes a secure, anonymous hotline for staff to report potential money-laundering concerns, with policies guaranteeing protection against adverse employment actions.

Challenges: Ensuring confidentiality, preventing misuse of the system, and fostering a culture where reporting is valued.

Adverse Media Screening – The process of scanning public and proprietary news sources for negative information about a customer or related party.

Related terms: negative news, reputational risk, automated screening.

Explanation: Detecting adverse media helps identify potential corruption, fraud, or sanctions violations that may not appear in official lists.

Practical application: An AML platform integrates a media monitoring service that flags clients appearing in news articles about fraud or bribery.

Challenges: Managing the volume of data, distinguishing relevant from irrelevant hits, and handling language and jurisdiction variations.

Beneficiary – The person or entity that ultimately receives the benefit of a transaction or asset.

Related terms: recipient, ultimate beneficial owner, payee.

Explanation: Identifying the beneficiary is crucial for understanding the purpose of a transaction and assessing associated risk.

Example: In a cross-border wire, the originating bank verifies the ultimate beneficiary to ensure the funds are not being diverted to a sanctioned individual.

Challenges: Complex payment chains, intermediary entities, and limited visibility in certain jurisdictions.

Compliance Culture – The collective attitudes, values, and behaviors that shape an organization’s approach to regulatory adherence.

Related terms: tone at the top, ethical standards, governance.

Explanation: A strong compliance culture promotes proactive risk management and reduces the likelihood of violations.

Practical application: Senior executives regularly communicate the importance of AML compliance, and performance metrics include compliance adherence.

Challenges: Changing entrenched attitudes, aligning incentives, and measuring cultural impact.

Economic Sanctions – Restrictions imposed by governments or international bodies to prohibit financial and commercial interactions with designated persons, entities, or countries.

Related terms: embargo, OFAC, UN resolutions, secondary sanctions.

Explanation: Violating sanctions can result in severe penalties, including fines and loss of market access.

Example: A bank refuses to process a transaction involving a company listed on the EU sanctions list, thereby avoiding potential regulatory breach.

Challenges: Rapidly changing sanction lists, overlapping jurisdictional requirements, and managing legitimate trade exceptions.

Financial Intelligence Unit (FIU) – A national agency responsible for receiving, analyzing, and disseminating financial information related to suspected money laundering or terrorist financing.

Related terms: SAR, AML reporting, inter-agency cooperation.

Explanation: FIUs act as the central hub for AML data, collaborating with law enforcement and international partners.

Example: An FIU receives a SAR from a bank and forwards relevant details to the national police for investigation.

Challenges: Ensuring data security, maintaining analytical capacity, and fostering timely information exchange.

High-Risk Customer – A client whose profile, business activities, or geographic exposure indicates a heightened likelihood of involvement in money laundering.

Related terms: risk rating, enhanced due diligence, red flags.

Explanation: High-risk customers require additional monitoring, stricter controls, and senior management oversight.

Example: A client operating in a jurisdiction identified as a FATF “high-risk jurisdiction” is classified as

high-risk and subjected to ongoing transaction reviews.

Challenges: Balancing risk mitigation with business development goals and avoiding discriminatory practices.

Internal Controls – Policies and procedures implemented within an organization to ensure operational effectiveness, compliance, and risk mitigation.

Related terms: governance, segregation of duties, audit.

Explanation: In AML, internal controls encompass client onboarding, transaction monitoring, reporting mechanisms, and employee training.

Practical application: A bank establishes a control matrix assigning responsibility for SAR filing to the compliance department, with independent audit checks.

Challenges: Designing controls that are both robust and adaptable to evolving threats.

Layering – The second stage of money laundering, involving a series of complex transactions to obscure the source of illicit funds.

Related terms: placement, integration, transaction complexity.

Explanation: During layering, funds are moved through multiple accounts, jurisdictions, or financial instruments to break the link to the original crime.

Example: Illicit proceeds are transferred through a series of offshore shell companies, each transaction masking the prior source.

Challenges: Detecting sophisticated layering schemes, especially when they involve digital assets or rapid, automated transfers.

Money-Laundering Detection System (MLDS) – Software tools that analyze transaction data to identify patterns indicative of laundering.

Related terms: rule-based engine, artificial intelligence, alert generation.

Explanation: MLDS combine rule sets, statistical models, and machine learning to improve detection accuracy and reduce false positives.

Practical application: An institution deploys a neural-network model that learns from historical SARs to prioritize high-risk alerts.

Challenges: Data quality, model interpretability, and the need for continuous tuning.

Negative News Screening – The practice of reviewing public information sources for adverse information about a client or counterpart.

Related terms: adverse media, reputational risk, automated alerts.

Explanation: Negative news can signal corruption, fraud, or sanctions violations that may not yet be reflected in official lists.

Example: An AML system flags a client whose name appears in a newspaper article about a bribery scandal, prompting a manual review.

Challenges: Volume of information, language barriers, and distinguishing credible reports from rumors.

Offshore Account – A bank account held in a jurisdiction different from the account holder’s residence, often in a low-tax or secrecy jurisdiction.

Related terms: tax haven, shell company, jurisdictional risk.

Explanation: Offshore accounts can facilitate anonymity and rapid cross-border movement of funds, raising AML concerns.

Example: A corporation opens an offshore account in a jurisdiction with limited information sharing, using it to receive payments from high-risk clients.

Challenges: Limited transparency, varying regulatory standards, and potential for misuse in illicit schemes.

Risk-Based Approach (RBA) – A methodology that allocates resources and controls proportionally to the level of risk identified.

Related terms: risk assessment, proportionality, mitigation.

Explanation: RBA allows institutions to focus on higher-risk customers, products, and geographies, optimizing compliance efficiency.

Practical application: A fintech firm applies a risk scoring model to determine which clients require EDD versus standard CDD.

Challenges: Accurately quantifying risk, avoiding regulatory criticism for insufficient controls, and maintaining flexibility as risk profiles shift.

Sanctions Evasion – Deliberate actions taken to circumvent economic sanctions, often by using intermediaries, third-party jurisdictions, or complex corporate structures.

Related terms: secondary sanctions, black-list, compliance breach.

Explanation: Evasion techniques may involve mislabeling goods, using front companies, or routing transactions through non-sanctioned entities.

Example: A trader masks a prohibited export by labeling it as a different commodity and routing the shipment through a non-sanctioned country.

Challenges: Detecting hidden relationships, ensuring due diligence on indirect parties, and staying current with evolving evasion tactics.

Sectoral Sanctions – Targeted restrictions that apply to specific industries or activities within a sanctioned country, rather than a blanket embargo.

Related terms: targeted sanctions, OFAC sectoral sanctions, compliance filtering.

Explanation: Sectoral sanctions may prohibit dealings with certain financial institutions, oil companies, or defense firms in a particular nation.

Practical application: A bank’s compliance system blocks transactions involving entities listed under the U.S. “30-day oil” sanction regime.

Challenges: Interpreting complex regulatory language and maintaining up-to-date lists of affected entities.

Source-of-Funds (SOF) Verification – The process of confirming the origin of the money a client uses to fund a transaction or account.

Related terms: source-of-wealth (SOW), documentation, risk assessment.

Explanation: SOF verification helps ensure that funds are not derived from illicit activities and supports AML risk profiling.

Example: A client provides audited financial statements, tax returns, and sale agreements to substantiate the source of a large deposit.

Challenges: Obtaining reliable documentation, privacy considerations, and assessing the credibility of self-reported information.

Suspicious Transaction – A transaction that deviates from a client’s normal behavior or exhibits characteristics commonly associated with money laundering.

Related terms: red flag, SAR, monitoring.

Explanation: Indicators may include unusually large amounts, rapid movement between accounts, or transactions involving high-risk jurisdictions.

Practical application: An AML analyst reviews a wire transfer that exceeds the client’s typical transaction size and originates from a country flagged for terrorism financing.

Challenges: Differentiating legitimate business activity from illicit behavior and managing the volume of alerts generated.

Trade Finance Risk – The potential for money-laundering or fraud inherent in trade-related financial products such as letters of credit, guarantees, and documentary collections.

Related terms: TBML, due diligence, documentary verification.

Explanation: Trade finance instruments can be manipulated to conceal illicit proceeds or to provide false documentation supporting fraudulent transactions.

Example: A bank scrutinizes a letter of credit by verifying the underlying shipment documents and checking the parties against sanction lists.

Challenges: Complex documentation, reliance on third-party banks, and limited visibility into the physical goods.

Virtual Currency – A digital representation of value that can be used as a medium of exchange, stored electronically, and transferred via peer-to-peer networks.

Related terms: cryptocurrency, blockchain, VASP.

Explanation: Virtual currencies pose AML challenges due to pseudonymity, rapid cross-border transfers, and the emergence of privacy-enhancing technologies.

Practical application: A regulated exchange implements blockchain analytics to trace the flow of funds and identify addresses associated with illicit activity.

Challenges: Keeping pace with new coin types, regulatory divergence, and ensuring effective KYC in a decentralized environment.

Wire Transfer Monitoring – The oversight of electronic funds transfers to detect suspicious patterns, such as rapid movements or connections to high-risk jurisdictions.

Related terms: SWIFT, transaction monitoring, SAR.

Explanation: Wire transfers are a common channel for moving illicit funds, requiring real-time or

near-real-time analysis.

Example: A bank's monitoring system flags a series of outbound wires to a country under sanctions, prompting immediate investigation.

Challenges: High transaction volumes, latency in data availability, and distinguishing legitimate business payments from illicit transfers.