
International Anti Money Laundering Standards

Regulatory Reporting and Recordkeeping Obligations

Anti-Money Laundering (AML)

Concept: The set of legal and regulatory measures designed to prevent the generation of illicit funds.

Related terms: KYC, CDD, FATF

Explanation: AML frameworks require institutions to identify, assess, and mitigate money-laundering risks through policies, procedures, and controls.

Example: A bank implements AML software to flag transactions exceeding a specified amount that match known typologies.

Practical application: Ongoing monitoring of client activity against risk profiles and reporting suspicious activity to authorities.

Challenges: Balancing thorough risk assessment with operational efficiency; keeping pace with evolving typologies.

Beneficial Owner

Concept: The natural person(s) who ultimately own or control a customer, directly or indirectly.

Related terms: Ownership structure, KYC, Register

Explanation: Identifying beneficial owners is essential for transparency, as they may be hidden behind corporate layers.

Example: A shell company registers a client; the AML officer must trace the ownership to the individual who holds a 25 % stake.

Practical application: Collecting and verifying identification documents for individuals who own 25 % or more of an entity.

Challenges: Inconsistent definitions across jurisdictions; reliance on third-party data that may be outdated.

Beneficial Ownership Register

Concept: A centralized repository that records the beneficial owners of legal entities.

Related terms: Beneficial Owner, Transparency, Public Register

Explanation: Many jurisdictions require entities to file beneficial ownership information, which regulators can access for AML purposes.

Example: The UK's People with Significant Control (PSC) register stores details of individuals with control over companies.

Practical application: Firms must update the register annually and notify changes within a specified timeframe.

Challenges: Data quality, privacy concerns, and cross-border information sharing.

Customer Due Diligence (CDD)

Concept: The process of verifying a customer's identity and assessing risk before establishing a business relationship.

Related terms: KYC, Enhanced Due Diligence, Risk-Based Approach

Explanation: CDD includes collecting identification documents, understanding the purpose of the relationship, and ongoing monitoring.

Example: A new corporate client provides articles of incorporation, a list of directors, and a shareholder register for verification.

Practical application: Automated CDD checks against sanctions lists and adverse media.

Challenges: High-volume onboarding, data inconsistencies, and resource-intensive verification for high-risk clients.

Enhanced Due Diligence (EDD)

Concept: Additional scrutiny applied to high-risk customers or transactions.

Related terms: CDD, Risk-Based Approach, PEP

Explanation: EDD may involve deeper background checks, source-of-funds verification, and senior-management approval.

Example: A politically exposed person (PEP) opens a high-value account; the institution conducts EDD to assess potential corruption risk.

Practical application: Using external investigative services to validate the legitimacy of funds.

Challenges: Time-consuming processes, higher compliance costs, and potential client friction.

Electronic Recordkeeping

Concept: Storing regulatory and compliance documents in digital formats.

Related terms: Record Retention, Data Security, Audit Trail

Explanation: Electronic systems must ensure data integrity, accessibility, and protection against tampering.

Example: A financial institution archives all SARs in an encrypted database with role-based access controls.

Practical application: Automated indexing of records to facilitate rapid retrieval during inspections.

Challenges: Cybersecurity threats, ensuring long-term readability of file formats, and meeting jurisdiction-specific storage requirements.

Financial Action Task Force (FATF)

Concept: An intergovernmental body that sets international AML and counter-terrorist financing standards.

Related terms: FATF Recommendations, Mutual Evaluation, AML

Explanation: FATF issues 40 Recommendations that serve as the global benchmark for AML compliance.

Example: A country adopts FATF's "risk-based approach" to tailor its AML controls to domestic threats.

Practical application: Regulators use FATF assessments to gauge a jurisdiction's compliance level.

Challenges: Translating broad recommendations into concrete national legislation; keeping pace with rapid regulatory changes.

Financial Intelligence Unit (FIU)

Concept: A national agency that receives, analyses, and disseminates financial information concerning suspicious transactions.

Related terms: SAR, AML, Reporting Obligations

Explanation: FIUs serve as the central hub for AML reporting, often providing feedback to reporting entities.

Example: In the United States, the Financial Crimes Enforcement Network (FinCEN) acts as the FIU.

Practical application: Firms submit SARs electronically via the FIU's portal, attaching supporting documentation.

Challenges: Varying reporting thresholds, differing data standards, and potential backlogs in FIU processing.

Financial Transaction Report (FTR)

Concept: A regulatory filing that details specific financial transactions meeting predefined criteria, such as large cash deposits.

Related terms: Threshold Reporting, SAR, AML Reporting

Explanation: FTRs are often required for cash transactions exceeding a statutory amount, enabling authorities to detect structuring.

Example: A casino reports a cash deposit of \$15,000 in an FTR to the FIU.

Practical application: Automated systems flag and generate FTRs when transactions cross the reporting threshold.

Challenges: Managing high volumes of reports, avoiding false positives, and ensuring accurate data entry.

Financial Transaction Monitoring

Concept: Ongoing analysis of customer transactions to detect patterns indicative of money laundering.

Related terms: Transaction Monitoring, AML Software, Alerts

Explanation: Monitoring systems apply rules-based or machine-learning models to generate alerts for further review.

Example: An automated system raises an alert when a client repeatedly transfers funds just below the \$10,000 reporting threshold.

Practical application: Real-time monitoring dashboards enable compliance officers to triage alerts efficiently.

Challenges: Alert fatigue, tuning rule parameters, and integrating data from multiple channels.

General Data Protection Regulation (GDPR)

Concept: A European Union regulation governing personal data protection and privacy.

Related terms: Data Retention, Privacy, AML

Explanation: GDPR imposes constraints on the processing and storage of personal data, affecting AML recordkeeping.

Example: An EU-based bank must ensure that AML records containing personal data are secured and retained only as long as necessary.

Practical application: Implementing data minimisation and pseudonymisation techniques in AML databases.

Challenges: Reconciling AML's long-term retention mandates with GDPR's "right to be forgotten" provisions.

Internal Controls

Concept: Policies and procedures designed to ensure compliance with AML regulations and mitigate operational risk.

Related terms: Governance, Risk Management, Compliance

Explanation: Effective internal controls encompass segregation of duties, regular training, and internal audits.

Example: A firm establishes a dual-approval process for high-value wire transfers to prevent unauthorized transactions.

Practical application: Periodic testing of controls using audit checklists and remediation of identified gaps.

Challenges: Maintaining control effectiveness amid rapid business growth and technology changes.

KYC (Know Your Customer)

Concept: The process of verifying the identity of a client and understanding the nature of their activities.

Related terms: CDD, AML, Customer Identification

Explanation: KYC is the foundational step in AML compliance, ensuring that institutions know who they are dealing with.

Example: Collecting a passport, proof of address, and a self-declaration of source of wealth from a new client.

Practical application: Digital KYC platforms enable remote onboarding through video verification and AI-driven document checks.

Challenges: Balancing thoroughness with client experience, especially for low-risk customers.

Lawful Basis for Reporting

Concept: The legal justification that permits a reporting entity to disclose client information to authorities.

Related terms: Confidentiality, AML Obligations, Regulatory Requirement

Explanation: AML statutes often provide an explicit exemption from confidentiality rules when filing reports.

Example: A bank submits a SAR despite a confidentiality clause in its client agreement, relying on statutory authority.

Practical application: Legal counsel reviews reporting policies to ensure compliance with both AML and privacy laws.

Challenges: Navigating conflicting obligations between AML reporting and professional secrecy statutes.

Money Laundering

Concept: The process of disguising the origins of illegally obtained funds to make them appear legitimate.

Related terms: AML, Terrorist Financing, Structuring

Explanation: Money laundering typically involves three stages: placement, layering, and integration.

Example: A drug trafficker deposits cash into a legitimate business, then transfers the proceeds through multiple offshore accounts.

Practical application: AML programs target each stage with specific controls, such as cash transaction monitoring for placement.

Challenges: Detecting sophisticated layering techniques that use complex corporate structures and digital currencies.

Money Laundering Reporting Officer (MLRO)

Concept: The senior individual responsible for overseeing an organization's AML compliance and reporting obligations.

Related terms: Compliance Officer, SAR, Internal Controls

Explanation: The MLRO ensures that suspicious activity is identified, investigated, and reported to the FIU.

Example: The MLRO reviews an alert generated by the transaction monitoring system and decides to file a SAR.

Practical application: The MLRO maintains a register of AML training, supervises internal audits, and liaises with regulators.

Challenges: Keeping abreast of regulatory updates, managing resource constraints, and handling high-risk client relationships.

National AML/CFT Strategy

Concept: A country's comprehensive plan to combat money laundering and terrorist financing.

Related terms: FATF, Regulatory Framework, Enforcement

Explanation: Strategies outline objectives, legislative reforms, and inter-agency coordination mechanisms.

Example: A jurisdiction publishes a five-year AML strategy that includes establishing a new FIU and strengthening penalties.

Practical application: Institutions align internal policies with national priorities to demonstrate compliance.

Challenges: Translating strategic goals into actionable regulations; ensuring consistent enforcement across agencies.

Operational Risk

Concept: The risk of loss resulting from inadequate or failed internal processes, people, systems, or external events.

Related terms: Internal Controls, AML, Compliance

Explanation: In AML, operational risk includes failures in transaction monitoring, reporting, or recordkeeping.

Example: A system outage prevents the timely filing of SARs, exposing the firm to regulatory penalties.

Practical application: Conducting risk assessments to identify vulnerabilities and implementing mitigation measures.

Challenges: Quantifying AML-related operational risk and integrating it with enterprise-wide risk frameworks.

PEP (Politically Exposed Person)

Concept: An individual who holds or has held a prominent public function, and their immediate family and close associates.

Related terms: EDD, Risk-Based Approach, Sanctions

Explanation: PEPs are considered higher risk due to potential for corruption and abuse of power.

Example: A former minister opens a corporate account; the institution conducts EDD to assess the source of wealth.

Practical application: Screening client databases against PEP lists and applying enhanced monitoring.

Challenges: Identifying indirect connections, such as family members living abroad, and maintaining up-to-date PEP data.

Regulatory Reporting

Concept: The mandatory submission of information to supervisory authorities as required by AML legislation.

Related terms: SAR, FTR, FIU

Explanation: Reports may include suspicious activity, large cash transactions, and compliance statistics.

Example: A bank files a quarterly AML compliance report detailing the number of SARs filed and the outcomes of investigations.

Practical application: Automated reporting tools generate required fields and transmit data securely to the regulator.

Challenges: Keeping abreast of changing reporting formats, ensuring data accuracy, and managing reporting deadlines.

Risk-Based Approach (RBA)

Concept: A methodology that tailors AML controls to the level of risk presented by customers, products, and jurisdictions.

Related terms: CDD, EDD, Risk Assessment

Explanation: RBA enables efficient allocation of resources by focusing on higher-risk areas.

Example: A bank applies simplified due diligence for low-risk retail customers while applying EDD for high-risk offshore entities.

Practical application: Risk scoring models assign numeric values to clients based on criteria such as geography and transaction volume.

Challenges: Developing robust risk metrics, avoiding over-reliance on static thresholds, and ensuring consistent risk calibration.

Sanctions List

Concept: A compilation of individuals, entities, and countries subject to economic or trade restrictions.

Related terms: AML, KYC, PEP

Explanation: Screening against sanctions lists is a core AML requirement to prevent prohibited transactions.

Example: An automated screening engine checks every new client against the United Nations and EU sanctions lists.

Practical application: Positive matches trigger alerts for further investigation before onboarding proceeds.

Challenges: High false-positive rates, frequent list updates, and differing jurisdictional sanctions regimes.

Source-of-Funds (SOF) Verification

Concept: The process of confirming the origin of the money used in a transaction or to fund an account.

Related terms: EDD, CDD, AML

Explanation: SOF verification helps ensure that funds are not derived from illicit activities.

Example: A client provides audited financial statements and tax returns to demonstrate the legitimacy of a \$5 million deposit.

Practical application: Collecting documentary evidence such as sale agreements, inheritance documents, or loan contracts.

Challenges: Evaluating the authenticity of documents, dealing with complex corporate structures, and language barriers.

Suspicious Activity Report (SAR)

Concept: A confidential filing made by a reporting entity to the FIU describing a transaction or activity that appears suspicious.

Related terms: SAR Filing, FIU, AML

Explanation: SARs are a primary tool for law enforcement to detect and investigate money-laundering schemes.

Example: An unusual pattern of rapid, high-value transfers to multiple jurisdictions triggers a SAR.

Practical application: Institutions maintain SAR logbooks, assign case numbers, and retain supporting documentation for prescribed periods.

Challenges: Determining when an activity is sufficiently suspicious, avoiding over-reporting, and protecting the confidentiality of the report.

Suspicious Transaction Report (STR)

Concept: Another term for SAR, used in certain jurisdictions to denote a report of suspicious activity.

Related terms: SAR, AML Reporting, FIU

Explanation: The content and filing requirements are generally identical to SARs, though nomenclature may differ.

Example: In the United Kingdom, a financial institution submits an STR to the National Crime Agency.

Practical application: Standardised templates capture details such as transaction date, amount, parties, and rationale for suspicion.

Challenges: Consistency in terminology across multinational firms and ensuring staff understand local filing obligations.

Threshold Reporting

Concept: The requirement to report transactions that exceed a predefined monetary value, regardless of suspicion.

Related terms: FTR, Cash Transaction, AML

Explanation: Thresholds are set to capture large cash movements that could indicate structuring or other illicit behavior.

Example: A casino must file a cash transaction report for any single cash deposit over \$10,000.

Practical application: Real-time monitoring systems automatically generate reports when thresholds are breached.

Challenges: Managing the volume of reports generated by high-traffic businesses and differentiating legitimate large transactions from suspicious ones.

Transaction Monitoring System (TMS)

Concept: Software that analyses transaction data to detect anomalies and potential money-laundering activity.

Related terms: Monitoring, Alerts, AML

Explanation: TMS employ rule-based logic, statistical models, or AI to generate alerts for review.

Example: A TMS flags a series of inbound transfers that are just below the \$10,000 reporting threshold, suggesting possible structuring.

Practical application: Configurable parameters allow institutions to adjust sensitivity based on risk appetite.

Challenges: Calibration of detection rules, integration with legacy banking systems, and minimizing false positives.

Unstructured Data in AML

Concept: Information that does not conform to a predefined data model, such as emails, PDFs, and free-text notes.

Related terms: Data Mining, AML Analytics, Recordkeeping

Explanation: Unstructured data can contain valuable clues about suspicious activity but requires advanced processing techniques.

Example: Text mining of email communications reveals discussions about “cleaning” funds.

Practical application: Deploying natural-language processing tools to extract entities and flag risk-relevant content.

Challenges: Ensuring data privacy, handling large volumes, and achieving accurate classification.

Virtual Asset Service Provider (VASP)

Concept: An entity that conducts activities related to virtual assets, such as exchanges, wallet providers, or custodians.

Related terms: AML, FATF, Crypto

Explanation: VASPs are subject to AML obligations, including customer identification, transaction monitoring, and reporting.

Example: A cryptocurrency exchange implements KYC checks and files SARs for suspicious token transfers.

Practical application: Integrating blockchain analytics tools to trace the flow of virtual assets.

Challenges: Pseudonymity of blockchain transactions, rapidly evolving technology, and regulatory fragmentation.

Whistleblower Protection

Concept: Legal safeguards that encourage individuals to report misconduct without fear of retaliation.

Related terms: SAR, Compliance, Confidentiality

Explanation: In many AML regimes, employees can confidentially disclose suspicious activity, and the regulator may provide anonymity.

Example: An employee uses the firm's internal hotline to report a colleague's involvement in a money-laundering scheme.

Practical application: Establishing secure reporting channels and policies that protect the identity of whistleblowers.

Challenges: Balancing confidentiality with the need for investigative detail, and ensuring reports are acted upon promptly.

Wire Transfer Reporting

Concept: The mandatory filing of information on international wire transfers that meet certain criteria, such as exceeding a monetary threshold.

Related terms: SAR, FIU, AML

Explanation: Wire transfer reports help detect cross-border money-laundering and terrorist financing.

Example: A bank files a wire transfer report for a \$25,000 outbound remittance to a high-risk jurisdiction.

Practical application: Automated generation of reports that include sender and beneficiary details, purpose of payment, and intermediary banks.

Challenges: Capturing accurate beneficiary information, dealing with multi-currency transactions, and complying with differing jurisdictional thresholds.

AML Audit Trail

Concept: A chronological record of all AML-related actions, decisions, and communications within an institution.

Related terms: Recordkeeping, Compliance, Audit

Explanation: An audit trail enables regulators to verify that AML policies were properly applied and that due diligence was performed.

Example: The system logs each step taken by an analyst when reviewing a SAR, including timestamps and user IDs.

Practical application: Maintaining immutable logs that can be exported for regulator-initiated examinations.

Challenges: Ensuring completeness of logs, protecting the integrity of the data, and managing storage costs.

AML Compliance Program

Concept: A structured set of policies, procedures, and controls designed to meet AML regulatory requirements.

Related terms: Internal Controls, MLRO, Risk Assessment

Explanation: A comprehensive program includes governance, training, monitoring, reporting, and periodic review.

Example: A multinational bank adopts a global AML policy, with local adaptations for each jurisdiction's specific rules.

Practical application: Conducting annual self-assessments to verify that all elements of the program remain effective.

Challenges: Coordinating across business lines, maintaining consistency while respecting local legal nuances, and securing senior-management commitment.

Anti-Bribery and Corruption (ABC) Controls

Concept: Measures aimed at preventing bribery and corrupt practices, often overlapping with AML controls.

Related terms: PEP, EDD, Corporate Governance

Explanation: ABC controls may include gift registers, third-party due diligence, and regular ethics training.

Example: A company implements a policy that requires approval for any gifts exceeding a modest monetary value.

Practical application: Integrating ABC risk assessments into the overall AML risk-based framework.

Challenges: Distinguishing between legitimate business hospitality and illicit inducements, especially in high-risk regions.

Beneficial Ownership Disclosure

Concept: The act of providing information about the natural persons who ultimately own or control a legal entity.

Related terms: Register, Transparency, AML

Explanation: Disclosure is required to combat opaque corporate structures that facilitate money laundering.

Example: A trust file includes the settlor's name, the protector's identity, and the beneficiaries' details.

Practical application: Using standardized templates to capture ownership data for regulatory filing.

Challenges: Complex ownership chains, privacy laws that restrict public disclosure, and the need for ongoing updates.

Compliance Culture

Concept: The collective attitude, values, and behaviors within an organization that promote adherence to AML regulations.

Related terms: Training, Tone-at-the-Top, Ethics

Explanation: A strong compliance culture encourages proactive risk identification and reporting.

Example: Employees feel comfortable escalating suspicious activity because senior management regularly discusses compliance successes.

Practical application: Embedding compliance metrics into performance evaluations and reward structures.

Challenges: Overcoming entrenched practices that prioritize revenue over risk, and ensuring culture is consistent across global sites.

Data Retention Schedule

Concept: A policy that defines how long AML-related records must be kept before disposal.

Related terms: Recordkeeping, GDPR, Archive

Explanation: Retention periods are often set by law, typically ranging from five to ten years, depending on jurisdiction.

Example: A bank retains SARs and supporting documents for seven years after filing.

Practical application: Automated archiving solutions enforce retention rules and securely delete expired records.

Challenges: Balancing legal obligations with data minimisation principles, and managing cross-border data transfers.

Digital Identity Verification

Concept: The use of electronic methods to confirm a person's identity, often through biometric or document authentication.

Related terms: KYC, E-Verification, AML

Explanation: Digital verification streamlines onboarding while maintaining compliance with AML standards.

Example: A fintech app captures a selfie and matches it to a government-issued ID using AI-driven facial recognition.

Practical application: Integrating verification APIs that provide real-time validation and risk scoring.

Challenges: Ensuring accuracy across diverse document types, preventing spoofing attacks, and complying with privacy regulations.

Electronic Funds Transfer (EFT) Monitoring

Concept: Surveillance of electronic transfers of money between accounts to detect suspicious patterns.

Related terms: Wire Transfer Reporting, TMS, AML

Explanation: EFT monitoring focuses on rapid, high-volume transactions that may conceal laundering activity.

Example: An EFT system flags a series of rapid inbound transfers from multiple unrelated accounts to a single beneficiary.

Practical application: Setting velocity thresholds and pattern-recognition rules within the monitoring platform.

Challenges: High data throughput, distinguishing legitimate business payments from illicit flows, and handling cross-border nuances.

Financial Crime Risk Assessment

Concept: A systematic evaluation of the likelihood and impact of various financial crime threats to an organization.

Related terms: RBA, AML, Operational Risk

Explanation: The assessment informs the design of controls, resource allocation, and monitoring intensity.

Example: A bank identifies high-risk regions, product lines, and customer types, assigning each a risk score.

Practical application: Updating the risk assessment annually and after major regulatory changes.

Challenges: Accurately quantifying emerging threats such as cyber-enabled money laundering, and integrating qualitative judgments.

Foreign Account Tax Compliance Act (FATCA)

Concept: A U.S. law requiring foreign financial institutions to report holdings of U.S. persons to the IRS.

Related terms: AML, Reporting Obligations, CRS

Explanation: While not an AML law per se, FATCA's reporting requirements intersect with AML recordkeeping.

Example: A European bank collects a self-certification from a client confirming non-U.S. status to comply with FATCA.

Practical application: Incorporating FATCA checks into the KYC workflow alongside AML screening.

Challenges: Managing dual compliance with FATCA and local AML regulations, and handling client resistance to additional documentation.

Global AML Standards

Concept: Internationally recognised principles and guidelines that harmonise anti-money-laundering efforts.

Related terms: FATF, AML, Compliance

Explanation: The standards provide a common framework for jurisdictions to develop effective AML regimes.

Example: Adoption of the FATF Recommendations as the basis for national AML legislation.

Practical application: Aligning internal policies with global best practices to facilitate cross-border transactions.

Challenges: Reconciling divergent national interpretations and ensuring consistent enforcement.

High-Risk Jurisdiction List

Concept: A designation of countries considered to have weak AML controls or significant money-laundering problems.

Related terms: Risk Assessment, Sanctions, PEP

Explanation: Entities from high-risk jurisdictions often trigger enhanced due diligence.

Example: A client incorporated in a jurisdiction on the FATF "high-risk" list requires additional verification of source-of-funds.

Practical application: Maintaining an up-to-date list within the screening engine and applying stricter monitoring rules.

Challenges: Frequent updates, political sensitivities, and the risk of over-screening legitimate businesses.

Integrated Compliance Management System (ICMS)

Concept: A unified platform that consolidates AML, sanctions, fraud, and regulatory reporting functions.

Related terms: TMS, SAR, Data Governance

Explanation: An ICMS enables streamlined workflows, single-source data, and consistent reporting.

Example: An institution uses an ICMS to generate SARs, manage case assignments, and produce regulatory dashboards.

Practical application: Role-based access controls ensure that only authorized users can view sensitive SAR information.

Challenges: Complex implementation, data migration from legacy systems, and ensuring system scalability.

International Sanctions Compliance

Concept: Adherence to economic and trade restrictions imposed by entities such as the United Nations, European Union, and United States.

Related terms: AML, OFAC, Screening

Explanation: Sanctions compliance is a critical component of AML programs, preventing prohibited transactions.

Example: A bank blocks a payment to an entity listed on the OFAC Specially Designated Nationals (SDN) list.

Practical application: Real-time screening of customers and transactions against multiple sanctions lists.

Challenges: Managing contradictory sanctions regimes, ensuring timely updates, and handling false positives that disrupt legitimate commerce.

Legal Entity Identifier (LEI)

Concept: A unique 20-character alphanumeric code that identifies legal entities participating in financial transactions.

Related terms: KYC, Transparency, AML

Explanation: LEIs facilitate the aggregation of data across jurisdictions and improve the quality of AML screening.

Example: A corporate client provides its LEI during onboarding, allowing the institution to cross-reference the entity against global databases.

Practical application: Incorporating LEI validation into the client data intake workflow.

Challenges: Ensuring clients obtain and maintain an LEI, and dealing with entities that lack an LEI in certain markets.

Money-Laundering Risk Matrix

Concept: A visual tool that plots risk factors (e.g., geography, product, client type) to aid in risk prioritisation.

Related terms: RBA, Risk Assessment, Heat Map

Explanation: The matrix helps compliance teams allocate resources to the most vulnerable areas.

Example: The matrix shows high risk for offshore trusts combined with high-value cash transactions, prompting targeted monitoring.

Practical application: Updating the matrix quarterly based on new intelligence and regulatory guidance.

Challenges: Subjectivity in assigning risk scores, and keeping the matrix aligned with dynamic threat landscapes.

Monitoring Thresholds

Concept: Pre-defined limits that trigger alerts when transaction amounts, frequencies, or patterns exceed normal expectations.

Related terms: TMS, Alerts, SAR

Explanation: Thresholds are calibrated to balance detection effectiveness with manageable alert volumes.

Example: A threshold of three cash deposits above \$5,000 within a 24-hour period generates an alert.

Practical application: Configuring thresholds per product line and adjusting them based on observed trends.

Challenges: Avoiding "alert fatigue," dealing with seasonal spikes, and ensuring thresholds reflect genuine

risk.

Operational AML Controls

Concept: Day-to-day procedures that enforce AML policies, such as transaction screening, recordkeeping, and reporting.

Related terms: Internal Controls, TMS, SAR

Explanation: Operational controls are the practical implementation of the AML compliance program.

Example: Front-office staff receive prompts to verify client identification whenever a transaction exceeds a set limit.

Practical application: Routine reconciliations of monitoring outputs against actual transaction logs.

Challenges: Maintaining consistency across channels, training staff on new controls, and integrating controls into legacy processes.

Periodic AML Review

Concept: A scheduled evaluation of AML policies, procedures, and effectiveness.

Related terms: Audit, RBA, Compliance

Explanation: Reviews identify gaps, assess the adequacy of controls, and recommend improvements.

Example: An annual internal audit assesses the completeness of SAR filings and the timeliness of reporting.

Practical application: Documenting review findings, action plans, and management sign-off.

Challenges: Resource constraints, keeping review scope aligned with evolving regulatory expectations, and ensuring corrective actions are implemented.

Regulatory Change Management

Concept: The systematic process of monitoring, assessing, and implementing changes to AML regulations.

Related terms: Compliance, Policy Update, Training

Explanation: Effective change management ensures that institutions remain compliant as laws evolve.

Example: A new AML directive raises the cash transaction reporting threshold; the firm updates its monitoring rules accordingly.

Practical application: Maintaining a regulatory watchlist, assigning responsibility for impact analysis, and communicating updates to relevant staff.

Challenges: Rapid legislative turnover, interpreting ambiguous language, and coordinating updates across multiple business units.

Risk Appetite Statement

Concept: A formal declaration of the level of risk an organization is willing to accept in pursuit of its objectives.

Related terms: RBA, Governance, AML

Explanation: In AML, the risk appetite guides the intensity of due diligence and monitoring.

Example: A bank declares a low risk appetite for high-risk jurisdictions, resulting in mandatory EDD for all related clients.

Practical application: Embedding the risk appetite into the risk assessment methodology and monitoring

parameters.

Challenges: Aligning risk appetite with business growth targets, and communicating the statement effectively to front-office personnel.

Sanctions Screening Frequency

Concept: The interval at which client and transaction data are compared against sanctions lists.

Related terms: Ongoing Monitoring, SAR, FIU

Explanation: Continuous screening is essential because sanctions lists are frequently updated.

Example: A financial institution performs daily sanctions screening for all new and existing customers.

Practical application: Automating the ingestion of list updates and re-screening affected records automatically.

Challenges: Managing high-volume re-screening without degrading system performance, and handling discrepancies between different list providers.

Sector-Specific AML Guidance

Concept: Tailored AML recommendations for particular industries, such as gambling, real estate, or cryptocurrency.

Related terms: FATF, Risk Assessment, Guidance

Explanation: Different sectors face unique money-laundering risks requiring specialised controls.

Example: Real-estate firms may implement source-of-wealth checks for large cash purchases of property.

Practical application: Developing sector-focused policies that incorporate industry-specific red flags.

Challenges: Keeping up with sector-specific regulatory updates and ensuring consistent application across diversified business lines.

Suspicious Activity Detection (SAD)

Concept: The analytical process of identifying patterns or behaviours that may indicate money-laundering.

Related terms: TMS, Alerts, SAR

Explanation: SAD combines rule-based detection with advanced analytics to surface potential illicit activity.

Example: An AI model flags a sudden surge in cross-border transfers that deviate from a client's historical profile.

Practical application: Deploying dashboards that visualise suspicious patterns for analyst review.

Challenges: Data quality, model explainability, and the need for human expertise to interpret complex alerts.

Transaction Aggregation

Concept: The consolidation of multiple related transactions into a single view for risk assessment.

Related terms: Monitoring, Structuring, SAR

Explanation: Aggregation helps detect structuring, where a client splits a large amount into smaller transactions to avoid reporting.

Example: Five cash deposits of \$9,500 each within a week are aggregated to reveal an underlying \$47,500 activity.

Practical application: Configuring monitoring systems to sum transactions by customer, product, and

time-frame.

Challenges: Determining appropriate aggregation windows, and avoiding excessive aggregation that masks legitimate activity.

Virtual Currency Transaction Reporting

Concept: The filing of reports concerning transactions involving virtual currencies that meet reporting thresholds.

Related terms: VASP, AML, SAR

Explanation: Many jurisdictions treat virtual currency transfers similarly to cash for AML reporting purposes.

Example: A crypto exchange files a report for a \$30,000 Bitcoin transfer to a wallet in a high-risk jurisdiction.

Practical application: Integrating blockchain analytics to automatically identify and report high-value transfers.

Challenges: Rapidly changing regulatory definitions of virtual assets, and the pseudonymous nature of blockchain transactions.

Whitelist Management

Concept: The process of maintaining a list of approved entities or individuals exempt from certain AML checks.

Related terms: Screening, Exceptions, Risk Management

Explanation: Whitelists reduce operational burden but must be carefully controlled to avoid abuse.

Example: A bank maintains a whitelist of long-standing corporate clients with proven clean records,