
Compliance and Anti Money Laundering

Ethics and Governance Office

Anti-Money Laundering (AML) – Related terms: KYC, Transaction Monitoring, Suspicious Activity Report (SAR).

Explanation: A set of laws, regulations, and procedures designed to prevent the conversion of illicit funds into legitimate assets. The Ethics and Governance Office (EGO) ensures that the organization's AML program aligns with statutory requirements and internal risk appetite.

Example: A bank detects a sudden influx of large cash deposits from a new client; the AML system flags the activity, prompting a SAR filing.

Practical application: Developing a risk-based AML policy, training staff, and conducting periodic reviews of detection rules.

Challenges: Keeping pace with evolving typologies, balancing customer experience with stringent controls, and managing cross-border regulatory differences.

Beneficial Owner – Related terms: Ownership Structure, Transparency, Customer Due Diligence (CDD).

Explanation: The natural person who ultimately owns or controls a legal entity, directly or indirectly.

Identifying beneficial owners is critical for the EGO to assess exposure to illicit activities.

Example: A shell company is registered in a jurisdiction with lax disclosure rules; the EGO requires additional documentation to reveal the true owner.

Practical application: Implementing enhanced CDD procedures for high-risk entities and maintaining an up-to-date register of beneficial owners.

Challenges: Inconsistent global definitions, reliance on third-party data, and resistance from clients citing privacy concerns.

Compliance Monitoring – Related terms: Auditing, Key Performance Indicators (KPIs), Continuous Improvement.

Explanation: Ongoing oversight of policies, procedures, and controls to verify that they operate effectively and meet regulatory expectations. The EGO uses monitoring to detect gaps before they become violations.

Example: Monthly dashboards show a decline in timely SAR filings, triggering a remedial action plan.

Practical application: Deploying automated monitoring tools, conducting spot checks, and reviewing exception logs.

Challenges: Data overload, ensuring monitoring coverage across decentralized units, and maintaining objectivity in self-assessment.

Corporate Governance – Related terms: Board of Directors, Ethical Culture, Accountability.

Explanation: The framework of rules, practices, and processes by which an organization is directed and controlled. The EGO supports governance by embedding ethical standards into decision-making.

Example: A board adopts a code of conduct that requires all senior executives to certify compliance with AML policies annually.

Practical application: Establishing clear reporting lines, defining roles and responsibilities, and integrating

governance metrics into performance reviews.

Challenges: Aligning governance structures with rapid business growth, managing conflicts of interest, and ensuring board engagement on compliance matters.

Customer Due Diligence (CDD) – Related terms: KYC, Enhanced Due Diligence (EDD), Risk Rating.

Explanation: The process of collecting and verifying information about a client to assess the risk they pose. CDD is a foundational element of the EGO's AML strategy.

Example: Before onboarding a new corporate client, the compliance team validates the entity's registration documents and cross-checks the ultimate beneficial owners.

Practical application: Implementing tiered CDD based on risk classification, using electronic identity verification, and maintaining records for the statutory retention period.

Challenges: Balancing thoroughness with onboarding speed, handling incomplete or falsified documentation, and adapting to new data-privacy regulations.

Data Privacy – Related terms: GDPR, Confidentiality, Data Protection Impact Assessment (DPIA).

Explanation: The legal and ethical handling of personal information to protect individuals' rights. The EGO must reconcile AML data collection with privacy obligations.

Example: When sharing transaction data with a Financial Intelligence Unit, the organization anonymizes non-relevant personal details to comply with privacy laws.

Practical application: Conducting DPIAs for new AML technologies, establishing data-minimization policies, and training staff on secure data handling.

Challenges: Navigating conflicting jurisdictional requirements, mitigating breach risks, and ensuring that privacy safeguards do not impede effective monitoring.

Due Diligence – Related terms: CDD, EDD, Risk Assessment.

Explanation: A comprehensive investigation into a party's background, financial standing, and compliance history before entering a business relationship.

Example: Prior to acquiring a fintech startup, the EGO reviews its AML controls, past SAR filings, and regulatory inspections.

Practical application: Using checklists, third-party risk databases, and site visits to verify information.

Challenges: Time-intensive processes, reliance on external data quality, and the need to update findings as circumstances evolve.

Financial Intelligence Unit (FIU) – Related terms: SAR, AML Reporting, International Cooperation.

Explanation: A national agency responsible for receiving, analyzing, and disseminating financial information related to suspected money laundering or terrorist financing. The EGO liaises with the FIU to fulfill reporting obligations.

Example: After detecting suspicious wire transfers, the compliance team submits a SAR to the domestic FIU, which then shares relevant intelligence with counterpart agencies abroad.

Practical application: Establishing secure channels for FIU communication, maintaining a SAR filing calendar, and tracking feedback from the FIU.

Challenges: Varying FIU response times, differing data submission formats, and managing confidentiality constraints.

Governance Framework – Related terms: Policies, Controls, Risk Appetite.

Explanation: The structured set of policies, procedures, and oversight mechanisms that guide an organization's ethical and regulatory conduct. The EGO designs and maintains this framework to ensure consistency across business units.

Example: A tiered approval matrix requires senior management sign-off for any deviation from standard AML procedures.

Practical application: Mapping processes to control objectives, assigning owners, and conducting periodic gap analyses.

Challenges: Integrating legacy systems, achieving organization-wide buy-in, and updating the framework in response to emerging threats.

High-Risk Customer – Related terms: Risk Rating, EDD, Politically Exposed Person (PEP).

Explanation: A client whose profile, business activities, or jurisdictional exposure indicates a greater propensity for illicit behavior. The EGO applies enhanced scrutiny to such customers.

Example: A corporation operating in a sanctioned country is flagged as high-risk, prompting a full EDD review before any transaction approval.

Practical application: Maintaining a risk matrix, automating alerts for high-risk indicators, and documenting mitigation steps.

Challenges: Determining appropriate risk thresholds, avoiding over-classification that strains resources, and managing client relationships sensitively.

Internal Controls – Related terms: Segregation of Duties, Control Environment, Monitoring.

Explanation: Policies and procedures designed to ensure the integrity of financial reporting, compliance, and operational effectiveness. The EGO assesses the adequacy of internal controls related to AML.

Example: A control requires dual approval for any transaction exceeding a set threshold, reducing the risk of unauthorized transfers.

Practical application: Conducting control self-assessments, testing control efficacy, and remediating identified weaknesses.

Challenges: Control fatigue, ensuring controls evolve with business models, and balancing control rigor with operational efficiency.

International Sanctions – Related terms: OFAC, UN Sanctions, Embargo.

Explanation: Restrictions imposed by governments or international bodies on dealings with specified individuals, entities, or countries. The EGO must screen all counterparties against current sanctions lists.

Example: A payment to a vendor in a sanctioned country is blocked by the AML screening engine, generating an alert for review.

Practical application: Integrating real-time sanctions feeds, updating screening parameters, and training staff on sanction-related risks.

Challenges: Rapidly changing sanction regimes, false positives from name-matching algorithms, and potential reputational fallout from inadvertent breaches.

KYC (Know Your Customer) – Related terms: CDD, Identity Verification, Risk Profiling.

Explanation: The process of verifying the identity of clients to prevent fraud, money laundering, and terrorist

financing. KYC is the first line of defense for the EGO's AML program.

Example: A new retail client provides a passport and utility bill, which are scanned and validated through an electronic KYC solution.

Practical application: Deploying digital KYC platforms, establishing verification thresholds, and storing documents securely.

Challenges: Managing diverse document standards across jurisdictions, mitigating fraud in synthetic identity creation, and ensuring ongoing verification for existing customers.

Legal Entity Identifier (LEI) – Related terms: Global Identifier, Regulatory Reporting, Transparency.

Explanation: A unique 20-character alphanumeric code assigned to legal entities participating in financial transactions. The LEI enhances traceability and risk assessment.

Example: The compliance system requires that all corporate counterparties provide a valid LEI before processing transactions.

Practical application: Validating LEIs against the Global LEI System, incorporating LEI data into AML risk models, and updating records periodically.

Challenges: Incomplete LEI coverage in certain sectors, cost of acquisition for small entities, and maintaining synchronization with the central database.

Money Laundering – Related terms: Placement, Layering, Integration.

Explanation: The process of disguising the origins of illicit funds to make them appear legitimate.

Understanding the three stages helps the EGO design effective detection controls.

Example: Criminal proceeds from drug sales are deposited into a series of accounts (placement), transferred through multiple jurisdictions (layering), and finally invested in real estate (integration).

Practical application: Mapping transaction patterns to the typology stages, training staff to recognize red flags, and calibrating detection rules accordingly.

Challenges: Sophisticated laundering techniques, rapid movement of funds through digital channels, and limited visibility into offshore structures.

Operational Risk – Related terms: Process Failure, Internal Fraud, Business Continuity.

Explanation: The risk of loss resulting from inadequate or failed internal processes, people, systems, or external events. AML compliance is a key component of operational risk management.

Example: A system outage prevents the AML screening engine from processing transactions, leading to a backlog of unchecked activity.

Practical application: Developing contingency plans, conducting regular system stress tests, and establishing clear escalation procedures.

Challenges: Predicting rare events, allocating sufficient resources for risk mitigation, and integrating operational risk with overall enterprise risk frameworks.

Politically Exposed Person (PEP) – Related terms: High-Risk Customer, EDD, Sanctions.

Explanation: An individual who holds or has held a prominent public function, or their immediate family and close associates, who may present higher corruption risks. The EGO applies heightened due diligence to PEPs.

Example: A senior government official seeks to open a corporate account; the compliance team conducts an

EDD review, checking for adverse media and sanctions matches.

Practical application: Using PEP databases, documenting risk assessments, and monitoring ongoing transactions for unusual activity.

Challenges: Identifying indirect connections, handling frequent changes in political status, and balancing privacy concerns with risk mitigation.

Risk Assessment – Related terms: Risk Rating, Heat Map, Controls.

Explanation: The systematic process of identifying, analyzing, and evaluating risks to determine their potential impact and likelihood. The EGO conducts AML risk assessments to prioritize resources.

Example: A risk matrix assigns a high score to transactions involving high-risk jurisdictions, prompting additional monitoring.

Practical application: Conducting annual risk assessments, updating risk registers, and aligning risk appetite with control intensity.

Challenges: Data quality issues, subjectivity in scoring, and keeping assessments current amid evolving threats.

Sanctions Screening – Related terms: OFAC List, Watchlist, Transaction Blocking.

Explanation: The automated process of comparing counterparties, goods, and services against designated sanctions lists to prevent prohibited dealings. The EGO oversees the effectiveness of screening solutions.

Example: A payment to a vendor is automatically halted because the vendor's name matches an entry on the OFAC SDN list.

Practical application: Configuring screening thresholds, reviewing false positives, and documenting remediation actions.

Challenges: Managing high false-positive rates, ensuring coverage of all relevant lists, and maintaining audit trails for regulatory examinations.

Transaction Monitoring – Related terms: Alert Generation, Pattern Recognition, SAR.

Explanation: Ongoing analysis of customer transactions to detect suspicious behavior that may indicate money laundering or other illicit activity. The EGO calibrates monitoring rules to balance detection and efficiency.

Example: An account that typically processes low-value payments suddenly initiates a series of large cross-border transfers, triggering an alert.

Practical application: Deploying machine-learning models, setting escalation procedures, and reviewing alerts on a daily basis.

Challenges: Alert fatigue, tuning models to reduce false positives, and integrating monitoring across multiple channels and products.

Whistleblower Protection – Related terms: Ethics Hotline, Confidential Reporting, Retaliation Safeguard.

Explanation: Policies and mechanisms that encourage employees to report misconduct without fear of reprisal. The EGO ensures that whistleblower channels are secure and that reports are investigated promptly.

Example: An employee uses the ethics hotline to disclose that a senior manager is overriding AML controls; the compliance team initiates an independent investigation.

Practical application: Providing anonymous reporting tools, training staff on protection rights, and tracking case outcomes.

Challenges: Maintaining confidentiality, preventing misuse of the system, and fostering a culture where reporting is viewed positively.

Anti-Bribery and Corruption (ABC) – Related terms: FCPA, UK Bribery Act, Gift Policy.

Explanation: A set of regulations and internal policies aimed at preventing bribery, kickbacks, and other corrupt practices. The EGO aligns ABC controls with AML efforts to address overlapping risks.

Example: A sales representative offers a small gift to a government official; the ABC policy requires disclosure and approval, preventing a potential violation.

Practical application: Conducting risk-based ABC assessments, implementing gift registries, and providing regular training.

Challenges: Cultural differences in gift-giving, monitoring third-party intermediaries, and ensuring consistent enforcement across global operations.

Beneficial Ownership Registry – Related terms: Transparency Initiative, Corporate Disclosure, AML.

Explanation: A centralized database that records the natural persons who ultimately own or control legal entities. The EGO uses registry data to enhance client risk profiling.

Example: A corporation's registration details are cross-checked against the national beneficial ownership registry, revealing undisclosed owners.

Practical application: Integrating registry APIs into onboarding workflows, updating records upon ownership changes, and reporting discrepancies to senior management.

Challenges: Variability in registry accessibility, data accuracy concerns, and regulatory gaps in jurisdictions lacking such registries.

Compliance Culture – Related terms: Ethical Tone, Leadership Commitment, Behavioral Standards.

Explanation: The collective attitudes, values, and practices that influence how employees perceive and act on compliance obligations. The EGO promotes a strong compliance culture through visible leadership and incentives.

Example: The CEO regularly addresses the importance of AML compliance in town-hall meetings, reinforcing the organization's commitment.

Practical application: Embedding compliance metrics in performance reviews, recognizing compliant behavior, and conducting climate surveys.

Challenges: Overcoming complacency, aligning incentives with compliance goals, and measuring intangible cultural shifts.

Data Analytics in AML – Related terms: Predictive Modeling, Visualization, Big Data.

Explanation: The application of statistical and computational techniques to identify patterns, anomalies, and trends that may indicate illicit activity. The EGO leverages analytics to refine detection capabilities.

Example: Using clustering algorithms to isolate groups of accounts that exhibit similar unusual transaction patterns.

Practical application: Building dashboards for real-time monitoring, training analysts on data-driven investigation methods, and validating model performance regularly.

Challenges: Ensuring data quality, avoiding algorithmic bias, and securing sensitive financial data during analysis.

Emerging Technologies – Related terms: Blockchain, AI, RegTech.

Explanation: New tools and platforms that transform the way compliance functions operate, offering opportunities for greater efficiency and risk mitigation. The EGO evaluates technology adoption against regulatory expectations.

Example: Deploying an AI-powered KYC solution that automates document verification and reduces onboarding time.

Practical application: Conducting pilot projects, performing technology risk assessments, and establishing governance over tech vendors.

Challenges: Managing technology-related operational risk, ensuring regulatory acceptance of novel solutions, and addressing skill gaps within the compliance team.

Financial Crime – Related terms: Money Laundering, Terrorist Financing, Fraud.

Explanation: A broad category encompassing illegal activities that involve the movement or use of money for illicit purposes. The EGO's mandate includes detecting and preventing all forms of financial crime.

Example: A coordinated scheme uses multiple accounts to funnel proceeds from cyber-theft into legitimate businesses.

Practical application: Integrating crime typologies into training, coordinating with law-enforcement agencies, and maintaining a comprehensive crime-watch database.

Challenges: Inter-agency information sharing barriers, rapidly evolving crime methods, and resource constraints for comprehensive coverage.

Governance, Risk, and Compliance (GRC) – Related terms: Integrated Framework, Policy Management, Risk Dashboard.

Explanation: A unified approach that aligns governance structures, risk management processes, and compliance activities to achieve strategic objectives. The EGO adopts GRC principles to streamline AML oversight.

Example: A single GRC platform hosts AML policies, tracks risk assessments, and logs audit findings, providing senior management with a consolidated view.

Practical application: Defining GRC roles, establishing data flows between risk and compliance modules, and automating policy updates.

Challenges: Ensuring system interoperability, avoiding duplication of effort, and securing executive sponsorship for cross-functional initiatives.

High-Volume Transaction Monitoring – Related terms: Bulk Processing, Real-Time Screening, Threshold Alerts.

Explanation: Specialized monitoring of large batches of transactions, often in high-frequency environments such as payments processing or securities trading. The EGO designs rules to detect anomalies without overwhelming analysts.

Example: A payment processor monitors millions of daily transactions, using statistical thresholds to flag spikes in activity for certain merchants.

Practical application: Implementing tiered alert prioritization, leveraging distributed computing, and conducting periodic batch reviews.

Challenges: Managing system performance, reducing false positives at scale, and maintaining regulatory compliance for high-speed processing.

Internal Audit – Related terms: Independent Review, Control Testing, Assurance.

Explanation: An objective evaluation of an organization's internal controls, risk management, and governance processes. The EGO coordinates with internal audit to validate AML effectiveness.

Example: Internal audit conducts a walkthrough of the SAR filing process, identifying gaps in documentation and recommending corrective actions.

Practical application: Scheduling audit cycles, sharing audit findings with compliance owners, and tracking remediation status.

Challenges: Aligning audit scope with dynamic compliance priorities, avoiding audit fatigue, and ensuring timely implementation of audit recommendations.

Joint Money Laundering and Terrorist Financing Risk Assessment – Related terms: Dual-Use Risk, Threat Matrix, Strategic Review.

Explanation: An integrated assessment that evaluates the likelihood and impact of both money laundering and terrorist financing activities, recognizing overlapping risk factors. The EGO employs a combined methodology to optimize resource allocation.

Example: A regional office assesses that its exposure to both illicit cash smuggling and extremist financing is high, prompting enhanced monitoring protocols.

Practical application: Developing a unified risk scoring model, training staff on dual-risk indicators, and reporting findings to senior leadership.

Challenges: Differentiating between money-laundering and terrorist-financing typologies, avoiding double-counting of risks, and satisfying distinct regulatory reporting requirements.

Key Performance Indicators (KPIs) for AML – Related terms: Metrics, Dashboard, Benchmarking.

Explanation: Quantitative measures used to evaluate the effectiveness and efficiency of AML programs. The EGO defines KPIs to monitor compliance health and drive continuous improvement.

Example: KPI: Percentage of SARs filed within the mandated 30-day window; the current rate is 92%, exceeding the target of 90%.

Practical application: Setting KPI thresholds, automating data collection, and reviewing KPI trends in quarterly governance meetings.

Challenges: Selecting meaningful metrics, preventing KPI manipulation, and balancing quantitative data with qualitative insights.

Legal and Regulatory Change Management – Related terms: Compliance Updates, Impact Analysis, Training Refresh.

Explanation: The systematic process of identifying, evaluating, and implementing changes arising from new or amended laws, regulations, and guidance. The EGO maintains a change-management program to keep AML controls current.

Example: A new amendment to the EU AML Directive requires additional verification of high-risk third-party

relationships; the compliance team updates procedures accordingly.

Practical application: Monitoring regulatory feeds, conducting gap analyses, and issuing updated policy notices to affected business units.

Challenges: Keeping pace with frequent legislative updates, ensuring consistent implementation across global sites, and allocating resources for ongoing education.

Money Laundering Reporting Officer (MLRO) – Related terms: Compliance Officer, SAR, Accountability.

Explanation: The senior individual responsible for overseeing the organization's AML program, including the filing of SARs and liaison with regulatory authorities. The MLRO reports to the Ethics and Governance Office and the board.

Example: The MLRO reviews a high-value transaction alert, determines that a SAR is required, and submits the report to the FIU within the statutory deadline.

Practical application: Maintaining a register of MLRO responsibilities, documenting decision-making rationale, and ensuring the MLRO has adequate authority and resources.

Challenges: Managing workload during periods of heightened alert volume, navigating conflicts of interest, and maintaining independence from business pressures.

Operational Due Diligence (ODD) – Related terms: Third-Party Risk, Vendor Management, Service Provider Assessment.

Explanation: The evaluation of the operational capabilities, controls, and compliance posture of third-party service providers. The EGO conducts ODD to mitigate AML risks arising from outsourced functions.

Example: Before engaging a cloud-based AML screening vendor, the compliance team assesses the provider's data security measures, audit reports, and regulatory certifications.

Practical application: Deploying questionnaires, performing onsite visits, and establishing contractual clauses for ongoing monitoring.

Challenges: Limited visibility into vendor processes, differing standards across jurisdictions, and ensuring contractual enforcement of compliance obligations.

Political Exposure Screening – Related terms: PEP Database, Risk Rating, Ongoing Monitoring.

Explanation: The continuous verification of client and counterparty data against updated lists of politically exposed persons to identify emerging risks. The EGO integrates screening into both onboarding and periodic review cycles.

Example: An existing client's profile is automatically refreshed quarterly; the system flags a newly added family member who is now a senior minister, prompting a review.

Practical application: Scheduling automated refreshes, documenting risk mitigation steps, and escalating high-risk findings to senior management.

Challenges: Managing the volume of updates, avoiding alert fatigue, and reconciling discrepancies between multiple PEP data sources.

Risk Appetite Statement – Related terms: Risk Tolerance, Board Guidance, Strategic Alignment.

Explanation: A formal declaration by senior leadership that defines the level and type of risk the organization is willing to accept in pursuit of its objectives. The EGO aligns AML risk thresholds with the overall risk appetite.

Example: The board approves a risk appetite that permits moderate exposure to high-risk jurisdictions, provided that enhanced controls are in place.

Practical application: Translating the statement into quantitative risk scores, communicating expectations to business units, and reviewing alignment annually.

Challenges: Ensuring the statement reflects realistic operational capabilities, preventing risk-taking behavior that exceeds approved limits, and updating the appetite in response to market changes.

Sanctions Evasion – Related terms: Circumvention, Secondary Sanctions, Compliance Breach.

Explanation: The deliberate act of disguising or rerouting transactions to avoid detection by sanctions enforcement authorities. The EGO monitors for evasion techniques such as shell entities and false invoicing.

Example: An exporter uses a third-party intermediary in a non-sanctioned country to route goods to a sanctioned destination, concealing the ultimate beneficiary.

Practical application: Implementing layered screening, conducting deep-dive investigations of flagged transactions, and training staff on common evasion tactics.

Challenges: Detecting sophisticated concealment methods, balancing trade facilitation with enforcement duties, and managing reputational risk from inadvertent breaches.

Sector-Specific AML Risks – Related terms: Industry Typologies, Tailored Controls, Risk Mapping.

Explanation: Unique money-laundering vulnerabilities associated with particular business sectors, such as real estate, gaming, or virtual assets. The EGO develops sector-focused controls to address these distinct threats.

Example: In the virtual asset sector, rapid transfers across blockchain networks present challenges for transaction traceability, requiring specialized analytics.

Practical application: Conducting sector risk workshops, customizing monitoring rules, and collaborating with industry bodies for best-practice sharing.

Challenges: Keeping abreast of emerging sector trends, allocating resources proportionally across diverse lines of business, and integrating sector-specific controls into a unified AML framework.

Suspicious Activity Report (SAR) – Related terms: AML Filing, FIU, Confidentiality.

Explanation: A mandatory report submitted to a financial intelligence authority when a transaction or pattern raises suspicion of illegal activity. The EGO oversees SAR preparation, submission, and record-keeping.

Example: An account exhibits a sudden surge in wire transfers to offshore jurisdictions with no apparent business purpose; the compliance analyst prepares a SAR detailing the observations.

Practical application: Using SAR templates, ensuring timely filing within regulatory deadlines, and maintaining secure archives for the required retention period.

Challenges: Determining the threshold for suspicion, avoiding over-reporting that strains regulatory relationships, and protecting SAR confidentiality from internal leaks.

Third-Party Risk Management – Related terms: Vendor Due Diligence, ODD, Contractual Controls.

Explanation: The process of identifying, assessing, and mitigating risks associated with external partners who may impact the organization's compliance posture. The EGO integrates AML considerations into the broader third-party risk framework.

Example: A correspondent bank is evaluated for its AML controls before establishing a new relationship, with findings influencing the risk rating and ongoing monitoring frequency.

Practical application: Maintaining a centralized third-party risk register, conducting periodic reviews, and embedding compliance clauses in contracts.

Challenges: Gathering reliable data from overseas partners, reconciling differing regulatory expectations, and ensuring consistent enforcement across the supply chain.

Transaction Thresholds – Related terms: Alert Rules, Risk Scoring, Escalation Matrix.

Explanation: Predetermined monetary values that trigger additional scrutiny or automatic alerts within AML monitoring systems. Thresholds are calibrated based on risk appetite and regulatory guidance.

Example: Any single wire transfer exceeding \$100,000 is automatically flagged for review by the compliance team.

Practical application: Setting dynamic thresholds that adjust for customer risk profiles, documenting rationale for threshold settings, and reviewing thresholds annually.

Challenges: Balancing sensitivity to detect illicit activity while minimizing false positives, adapting thresholds to currency fluctuations, and ensuring thresholds align with global regulatory expectations.

Virtual Asset Service Provider (VASP) – Related terms: Crypto Exchange, AML/KYC, FATF Guidance.

Explanation: An entity that conducts activities related to virtual assets, such as exchange, wallet provision, or custodial services, and is subject to AML obligations. The EGO extends its compliance program to cover VASPs.

Example: A cryptocurrency exchange implements KYC checks, monitors blockchain transactions for suspicious patterns, and files SARs when necessary.

Practical application: Integrating blockchain analytics tools, establishing AML policies specific to virtual assets, and training staff on emerging crypto-related risks.

Challenges: Rapidly evolving technology, regulatory uncertainty in many jurisdictions, and the pseudonymous nature of many virtual asset transactions.

Whistleblower Policy – Related terms: Ethics Hotline, Protection Measures, Reporting Channels.

Explanation: A formal document that outlines the procedures, rights, and responsibilities for individuals who report suspected wrongdoing. The EGO ensures the policy complies with legal standards and promotes a safe reporting environment.

Example: The policy states that employees may submit concerns anonymously via an encrypted portal, and that retaliation is strictly prohibited.

Practical application: Communicating the policy through training sessions, monitoring usage of reporting channels, and conducting independent investigations of reported concerns.

Challenges: Encouraging utilization without fear, safeguarding the confidentiality of reports, and managing potential false or malicious allegations.