Customer Due Diligence

Ongoing Monitoring Unit

Anti-Money Laundering (AML)
Related terms: Customer Due Diligence, Financial Crime, Risk Assessment, Regulatory Compliance.
Explanation: AML refers to the set of laws, regulations and procedures designed to prevent the generation of income through illegal actions. In the context of the Ongoing Monitoring Unit (OMU), AML provides the legal framework that obliges institutions to continuously scrutinise customer activity for signs of illicit behaviour. Practical application includes the integration of transaction monitoring software that flags patterns consistent with money-laundering typologies. A common challenge is balancing the need for thorough surveillance with the risk of generating excessive false positives, which can overwhelm compliance staff and erode customer experience. Effective OMU operations rely on calibrated risk models that adjust thresholds based on customer risk profiles, transaction volumes and jurisdictional risk.

Beneficial Owner
Related terms: Ownership Structure, Shareholder, Control Person, Transparency.
Explanation: A beneficial owner is the natural person who ultimately owns or controls a legal entity, directly or indirectly. The OMU must identify and verify beneficial owners during the initial Customer Due Diligence (CDD) stage and continuously monitor any changes. For example, a corporate client that restructures its shareholding may introduce a new ultimate owner who is subject to sanctions. The OMU tracks public registries, corporate filings and third-party data to detect such shifts. Challenges arise when ownership is layered through multiple jurisdictions, making it difficult to trace the true controlling individual. In such cases, the OMU may employ enhanced due diligence (EDD) techniques, including direct inquiries and the use of specialised ownership-mapping tools.

Customer Due Diligence (CDD)
Related terms: Risk Assessment, Enhanced Due Diligence, KYC, Onboarding.
Explanation: CDD is the process of collecting and analysing information about a customer to assess the risk they pose to the institution. The OMU builds on the initial CDD findings to create a dynamic risk profile that is updated with each new transaction or interaction. For instance, a high-net-worth individual who suddenly begins transacting large sums in high-risk jurisdictions will trigger a review. The OMU's role is to ensure that any deviation from the baseline risk triggers appropriate alerts, investigations and, if necessary, escalation to senior compliance. A key difficulty is maintaining data quality over time; outdated or incomplete information can lead to missed alerts or unnecessary investigations.

Data Quality Management
Related terms: Data Governance, Master Data, Data Cleansing, Integrity.
Explanation: Data quality management ensures that the information used by the OMU is accurate,

complete, and timely. High-quality data enables reliable risk scoring and reduces the incidence of false alerts. Practical steps include regular data reconciliation between internal systems and external sources, such as sanctions lists and credit bureaus. An example of a challenge is dealing with inconsistent naming conventions across legacy systems, which can cause duplicate records or missed matches. The OMU often employs fuzzy-matching algorithms and standardisation rules to mitigate these issues, but must carefully calibrate thresholds to avoid over-matching legitimate customers.

Enhanced Due Diligence (EDD)
Related terms: High-Risk Customer, Politically Exposed Person, Risk Mitigation, Deep Dive.
Explanation: EDD is a more intensive form of CDD applied to customers who present a higher risk of financial crime. The OMU initiates EDD when risk indicators such as a Politically Exposed Person (PEP) status, involvement in high-risk sectors, or transactions in sanctioned regions are detected. Practical application includes obtaining additional documentation (e.g., source-of-wealth statements), conducting on-site visits, and performing deeper background checks. A frequent challenge is the resource intensity of EDD; it requires dedicated analyst time and may delay onboarding. The OMU mitigates this by employing risk-based triage, focusing resources on the most critical cases while using automated tools for lower-risk enhancements.

Financial Action Task Force (FATF)
Related terms: International Standards, Recommendations, AML/CTF, Jurisdictional Risk.
Explanation: FATF is an inter-governmental body that sets global standards for combating money laundering and terrorist financing. Its Recommendations serve as the benchmark for national AML regimes. The OMU aligns its monitoring policies with FATF guidance, such as the risk-based approach and the requirement to maintain up-to-date sanctions screening. Practical use includes referencing FATF typologies when configuring rule-sets in transaction monitoring systems. A challenge is that FATF updates its standards periodically, requiring the OMU to revise policies and re-train staff, which can be costly and time-consuming.

Geographic Risk
Related terms: Jurisdictional Risk, Sanctions, High-Risk Country, Political Stability.
Explanation: Geographic risk assesses the likelihood that a customer's location or the location of a transaction exposes the institution to higher AML/CTF risk. The OMU incorporates geographic risk scores into its overall risk model. For example, transactions involving a country subject to United Nations sanctions automatically generate higher risk scores and may be blocked pending review. Challenges include keeping abreast of rapidly changing geopolitical events, such as the imposition of new sanctions or the emergence of conflict zones, which require real-time updates to the OMU's risk parameters.

High-Risk Customer
Related terms: Risk Rating, EDD, Monitoring Frequency, Red Flag.
Explanation: A high-risk customer is one whose profile, activity or affiliations suggest a greater likelihood of involvement in financial crime. The OMU identifies high-risk customers using a combination of static

attributes (e.g., PEP status) and dynamic behaviour (e.g., sudden spikes in transaction volume). Practical application includes assigning a higher monitoring frequency, tighter transaction limits, and mandatory senior-level approvals for certain activities. A major challenge is avoiding "risk fatigue" where analysts become desensitised to alerts due to an overabundance of high-risk designations. The OMU addresses this by refining risk models to differentiate truly elevated risk from marginally higher risk, thereby preserving analyst focus.

Identity Verification
Related terms: KYC, Document Authentication, Biometrics, Onboarding.
Explanation: Identity verification confirms that a customer is who they claim to be, using reliable documents or electronic methods. In the OMU, identity verification data is stored and referenced during ongoing monitoring to detect inconsistencies, such as a mismatch between a previously verified address and a new address supplied in a transaction. Example: a customer who initially provided a passport from Country A later submits a driver's licence from Country B; the OMU flags this as a potential identity-theft indicator. Challenges include dealing with forged documents and the need for multi-factor verification methods, which increase operational complexity and cost.

International Sanctions Lists
Related terms: OFAC, UN Sanctions, Watchlist, Blocking.
Explanation: Sanctions lists contain the names of individuals, entities and regimes that are prohibited from receiving financial services. The OMU must continuously screen customers and transactions against these lists. Practical application involves automated matching engines that compare customer names, aliases, and associated entities against the latest list versions. If a match occurs, the OMU triggers a blocking or escalation workflow. A key challenge is dealing with name variations, transliteration issues, and false positives, which require skilled analysts to perform manual reviews and determine the appropriate regulatory response.

Key Risk Indicators (KRIs)
Related terms: Metrics, Dashboard, Thresholds, Early Warning.
Explanation: KRIs are quantifiable measures that signal changes in risk exposure. The OMU tracks KRIs such as the number of high-value transfers per customer, the frequency of cross-border payments, and the proportion of transactions to high-risk jurisdictions. By visualising KRIs on a compliance dashboard, the OMU can quickly identify emerging trends. For instance, a sudden increase in a customer's outbound transfers to a newly sanctioned country would raise a KRI alarm. Challenges include selecting KRIs that are truly predictive rather than merely descriptive, and ensuring that data feeds are reliable and timely.

Know Your Customer (KYC)
Related terms: CDD, Identity Verification, Onboarding, Customer Profile.
Explanation: KYC is the process of collecting basic identification information from customers at the start of a business relationship. While KYC is primarily an onboarding activity, its data feeds directly into the OMU's risk engine. The OMU uses KYC details such as occupation, source of funds, and anticipated transaction

patterns to establish baseline expectations. If actual behaviour deviates significantly, the OMU generates alerts for further investigation. A challenge is maintaining KYC data freshness; customers may change addresses or employment status without notifying the institution, leading to outdated risk assessments.

Legislative Reporting Requirements
Related terms: SAR, STR, Regulatory Filing, Compliance Timeline.
Explanation: These are the statutory obligations that require financial institutions to report suspicious activity to authorities. The OMU is responsible for detecting suspicious patterns and preparing Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs). Practical steps include documenting the rationale for the alert, the investigative actions taken, and the final recommendation. Challenges include strict filing deadlines, confidentiality constraints, and the risk of regulatory penalties for non-compliance or over-reporting. The OMU must balance thorough documentation with operational efficiency to meet reporting obligations.

Money Laundering Typologies
Related terms: Structuring, Smurfing, Trade-Based Money Laundering, Layering.
Explanation: Typologies are common methods used by criminals to disguise illicit proceeds. The OMU incorporates typology knowledge into its rule-sets and machine-learning models. For example, structuring (or “smurfing”) involves breaking large cash deposits into multiple small amounts to evade reporting thresholds; the OMU detects this by analysing deposit patterns over time. A challenge is that criminals continuously evolve their methods, requiring the OMU to stay current with emerging typologies through ongoing training and external intelligence sources.

Operational Risk
Related terms: Process Failure, System Outage, Human Error, Business Continuity.
Explanation: Operational risk refers to the possibility of loss resulting from inadequate or failed internal processes, people, systems or external events. In the OMU, operational risk manifests as missed alerts due to system downtime, data entry errors, or insufficient staffing. Practical mitigation includes redundant monitoring platforms, regular system health checks, and robust incident-response procedures. A recurring challenge is budgeting for sufficient resources while maintaining cost-effectiveness, especially in organisations where compliance is viewed as a cost centre rather than a strategic function.

Politically Exposed Person (PEP)
Related terms: Senior Official, Close Associate, Risk Rating, EDD.
Explanation: A PEP is an individual who holds or has held a prominent public function, along with their immediate family and close associates. Because of their access to public funds and potential for influence, PEPs are considered higher risk. The OMU flags any customer identified as a PEP during initial CDD and applies continuous monitoring, including periodic reviews of source-of-wealth documentation. For example, a PEP who begins receiving large, unexplained wire transfers from offshore entities would trigger an EDD review. Challenges include distinguishing legitimate transactions from illicit ones, especially when PEPs engage in complex investment structures.

Regulatory Change Management
Related terms: Policy Update, Impact Assessment, Training, Compliance Calendar.
Explanation: This discipline ensures that the OMU adapts its processes, systems and documentation to reflect new or amended regulations. Practical steps involve conducting impact analyses, updating monitoring rules, and delivering targeted training to analysts. A typical challenge is the speed at which regulators release guidance; the OMU must react quickly to avoid non-compliance gaps, which can strain resources and increase the likelihood of errors during transition periods.

Risk-Based Approach (RBA)
Related terms: Risk Assessment, Tiered Monitoring, Resource Allocation, Proportionality.
Explanation: RBA is the methodology of allocating monitoring effort according to the assessed risk of each customer or transaction. The OMU uses RBA to determine which accounts receive higher scrutiny, more frequent reviews, or enhanced analytics. For instance, a low-risk retail customer with stable transaction patterns may be monitored with basic rule-based checks, while a corporate client with complex cross-border flows receives advanced behavioural analytics. Challenges include ensuring that risk models are transparent, auditable and not overly reliant on historical data that may not predict future behaviour.

Sanctions Screening
Related terms: Watchlist Matching, Blocking, False Positive, Compliance Engine.
Explanation: Sanctions screening is the process of comparing customer names and transaction details against sanctioned parties lists. The OMU integrates screening engines that perform real-time checks on inbound and outbound payments. Practical example: a wire transfer destined for a bank in a country under OFAC sanctions is automatically halted pending manual verification. A major challenge is managing the trade-off between detection accuracy and operational burden; overly aggressive screening can generate many false positives, while lax settings may miss prohibited parties. The OMU continuously fine-tunes matching thresholds and employs manual review queues to balance these concerns.

Transaction Monitoring
Related terms: Rule-Based Alerts, Behavioural Analytics, Real-Time Screening, Alert Management.
Explanation: Transaction monitoring is the core activity of the OMU, involving the systematic review of customer transactions to detect anomalies. The OMU deploys a combination of rule-based filters (e.g., transactions exceeding $10,000) and advanced analytics (e.g., clustering of similar patterns). An example of a rule-based alert is a sudden large cash deposit that exceeds a customer's typical volume. Behavioural analytics might identify a pattern of rapid fund movement through multiple accounts that resembles layering. Challenges include handling high volumes of alerts, ensuring timely investigation, and preventing alert fatigue among analysts.

Unusual Activity Report (UAR)
Related terms: SAR, Internal Escalation, Documentation, Regulatory Submission.
Explanation: A UAR is an internal document that records the detection of potentially suspicious activity before it is formally reported to regulators. The OMU uses UARs to capture investigative steps, evidence

gathered, and the decision rationale. Practical usage includes logging the date of detection, the specific rule triggered, and any follow-up actions taken. A challenge is ensuring that UARs are comprehensive yet concise, as overly verbose reports can delay escalation, while insufficient detail may result in regulatory scrutiny.

Virtual Asset Service Provider (VASP)
Related terms: Cryptocurrency, Blockchain, AML, Risk Assessment.
Explanation: VASPs are entities that facilitate the exchange, transfer or storage of virtual assets such as cryptocurrencies. The OMU treats VASPs as high-risk customers because of the pseudonymous nature of blockchain transactions. Practical monitoring includes tracing wallet addresses, analyzing transaction graphs, and screening against crypto-specific sanctions lists. A common challenge is the rapid evolution of blockchain technology, which creates new transaction types (e.g., decentralized finance protocols) that may fall outside existing monitoring rules, requiring the OMU to develop specialised analytics.

Watch-List Management
Related terms: Data Refresh, List Reconciliation, Source Validation, Alert Generation.
Explanation: Watch-list management involves the acquisition, validation and continual updating of sanction and PEP lists used by the OMU. The OMU must ensure that the latest versions of lists are loaded into screening engines without disruption. Practical steps include scheduled data feeds, checksum verification, and change-log analysis to identify new entries. Challenges include reconciling discrepancies between multiple list providers, handling differing data formats, and mitigating downtime during list updates, all of which can affect the OMU's ability to generate timely alerts.

Workflow Automation
Related terms: Business Process Management, Alert Triage, Case Management, Integration.
Explanation: Workflow automation streamlines the sequence of tasks an analyst performs when handling an alert. The OMU implements automated routing of alerts based on risk level, assignment to appropriate teams, and escalation triggers for senior review. For example, a low-risk alert may be auto-closed after a quick rule check, while a high-risk alert is automatically assigned to a senior analyst with a predefined investigation checklist. Challenges include ensuring that automation does not obscure decision-making, maintaining audit trails, and adapting workflows to accommodate new regulatory requirements without extensive re-coding.

Zero-Tolerance Policy
Related terms: Compliance Culture, Enforcement, Penalty, Governance.
Explanation: A zero-tolerance policy is an organizational stance that any breach of AML/CTF regulations, no matter how minor, will be met with strict corrective action. In the OMU, this policy drives rigorous monitoring, immediate escalation of alerts, and swift remedial measures. Practical implications include mandatory training refreshers after any incident and the implementation of disciplinary procedures for non-compliant behaviour. A challenge is preventing a culture of over-reporting, where staff generate unnecessary alerts to avoid perceived penalties, thereby increasing workload and diluting the focus on truly

high-risk cases. The OMU must balance strict enforcement with pragmatic risk management.