Standard Operating Procedure (SOP): Surveillance Obligations & Alert Processing

1. Objective & Scope

- **Objective:** To establish a structured workflow for detecting, analyzing, tracking, and reporting suspicious or manipulative market activities, ensuring complete compliance with SEBI and Exchange surveillance directives.
- **Scope:** Applies to all client trading activities (Cash and Derivatives segments) and Depository Participant (DP) account transactions.

2. Core Operational Workflow

1.Alert Ingestion & Logging: Day 1 (Daily/Real-time).

Download regulatory transactional alerts from Exchange Member Portals (NSE/BSE) and Depositories (CDSL/NSDL). Simultaneously, parse alerts generated via internal automated trading/DP systems. Log all alerts chronologically into a centralized **Surveillance Alert Register**.

2.First-Level Analysis (Maker): Within 10-15 Days of Generation.

The Alert Processor (Maker) reviews the transaction against the client's historical patterns, reported income, net worth, and known group associations. Cross-reference IP addresses for online trades and check for sudden spikes in illiquid scrips or volume concentration.

3.Client Inquiry & Evidence Gathering: As Required.

Where trading/transfer behavior is anomalous, reach out to the client to request a formal **trading rationale** and supporting financial documentation (e.g., bank statements, demat holding statements, contract notes from other brokers).

4.Secondary Verification (Checker): Before Day 30.

The Compliance Team (Checker) validates the Maker's findings and client-provided proofs. They categorize the disposition into two clear paths: **Verified & Closed** (rationale is genuine) or **Adverse Observation/Escalation** (potential market abuse or fraud).

5.Regulatory Reporting: Strictly within 30 or 45 Days.

Update the final disposition status on the Exchange Member Surveillance Dashboard or Depository portal. For Exchange-downloaded alerts, close within **45 days**. For Depository-provided alerts, submit within **30 days**. Report internally identified adverse alerts to the Exchange within **7 days** of internal conclusion.

3. Key Surveillance Alert Matrix

The surveillance desk actively monitors and cross-references transaction data with Client Due Diligence (CDD) across key risk patterns:

Trading Surveillance (Cash & Derivatives)

- **Volume & Price Anomalies:** Sudden trading activity in dormant accounts, or a single client/group accounting for a significant percentage of market volume in a specific scrip.
- **Manipulative Patterns:** Reversal of trades in derivatives, order book spoofing (placing large orders away from the market price to manipulate order books), circular trading, and pump-and-dump schemes.
- **Concentration Risks:** High open interest (OI) or concentrated turnover in illiquid options or specific stock futures contracts.
- **Financial Disproportionality:** Trading turnover or open positions that are completely non-commensurate with the client's declared annual income or audited net worth.

Depository Participant (DP) Surveillance

- **Demographic Alignment:** Multiple demat accounts opened with the same PAN, mobile number, email ID, or bank account.
- **High-Value Transfers:** Frequent or high-value off-market transfers executed immediately after a modification in critical KYC data (e.g., change of address, mobile number, or email).
- **Suspicious Reasons:** Frequent off-market transfers categorized under "Gifts" or "Donations" to unrelated third parties, or off-market sales executed outside the exchange mechanism.
- **Dormancy Triggers:** Newly opened demat accounts that witness an immediate, massive surge in transaction value followed by an abrupt shift back to zero holdings or dormancy.

4. Documentation & Corporate Governance

Record Retention Mandate: Background documents, client correspondence, bank/demat statements, and written observation summaries for every processed alert must be securely preserved for a minimum period of **8 years** under PMLA and SEBI guidelines.

Periodic Management Reporting

- **Daily Dashboard:** A daily operational summary of incoming and closed alerts must be presented to the Compliance Officer and Principal Officer.

- **Quarterly Board MIS:** A comprehensive Management Information System (MIS) report must be placed before the Board of Directors / Designated Directors within **15 days of the end of each quarter**.

MIS Reporting Parameter	Description
Opening Balance	Alerts pending analysis from the previous quarter.
New Inflow	Total alerts generated/downloaded during the current quarter.
Disposed Alerts	Number of alerts successfully verified, closed, or reported to authorities.
Closing Balance & Aging	Pending alerts, detailed aging analysis, and explicit reasons for any delay beyond the 30/45-day statutory limit.

5. Staffing & Qualifications

- All mid and senior-level staff members handling client onboarding, KYC, and transaction monitoring must clear the mandatory **NISM Certification** (e.g., NISM-Series-VII: Securities Operations and Risk Management, or relevant AML/KYC e-learning programs).
- The entire process operates under the direct oversight of the **Compliance Officer / Principal Officer**, who acts as the ultimate authority for regulatory escalations.