Standard Operating Procedure (SOP) for DP Surveillance Alerts Generation and Processing

1. Purpose This SOP outlines the process for generating and processing Depository Participant (DP) surveillance alerts to ensure compliance with regulatory requirements and to detect any suspicious or fraudulent activities.

2. Scope This procedure applies to all surveillance activities related to DP transactions, covering the generation, review, and resolution of alerts.

3. Responsibilities

- **Surveillance Team**: Responsible for monitoring and analysing alerts.
- **Compliance Team**: Ensures regulatory adherence and reviews escalated alerts.
- **IT Support**: Maintains and updates the surveillance system.
- **Senior Management**: Oversees the effectiveness of the surveillance process.

4. Alert Generation

- The surveillance system automatically generates alerts based on predefined rules and thresholds set by regulatory bodies and internal risk management teams.
- Common triggers include:
    - Unusual transaction volumes.
    - Frequent off-market transfers.
    - Transactions with no clear economic rationale.
    - Multiple trades in illiquid securities.
    - Transactions involving high-risk clients or entities.

5. Alert Review Process

- **Step 1: Initial Screening**
    - The Surveillance Team reviews alerts in the system.
    - Basic checks include transaction type, client profile, and historical patterns.
- **Step 2: Detailed Analysis**
    - Additional scrutiny is applied to high-risk alerts.
    - Supporting documents and client interactions are reviewed.
- **Step 3: Escalation**
    - If suspicious activity is confirmed, the alert is escalated to the Compliance Team.
    - Compliance may conduct further investigation or request additional information.

6. Resolution & Closure

- Alerts are categorized as:
    - **False Positives**: Closed with documentation.
    - **Genuine Alerts**: Escalated for further action.
- Compliance Team documents findings and, if required, reports the case to regulatory authorities.
- Closure of alerts is logged with appropriate remarks and supporting evidence.

7. Reporting & Record Keeping

- All alerts, actions taken, and resolutions are documented and stored securely.
- Periodic reports are generated for review by senior management.
- Regulatory reports are filed as per compliance requirements.

8. System Maintenance & Review

- Regular updates and enhancements to alert parameters are conducted based on trends and regulatory changes.
- Periodic audits ensure the efficiency and effectiveness of the surveillance process.

9. Training & Awareness

- Regular training sessions for staff involved in surveillance activities.
- Awareness programs to keep employees informed of emerging risks and compliance updates.

10. Compliance & Regulatory Requirements

- Adherence to guidelines issued by regulatory bodies such as SEBI, RBI, and relevant exchanges.
- Periodic compliance audits and self-assessments.

11. Exception Handling

- Any deviations from the SOP must be documented and approved by senior management.
- Emergency measures can be implemented in case of system failures or significant security threats.

This SOP ensures a structured approach to DP surveillance, enhancing regulatory compliance and mitigating risks associated with fraudulent or suspicious transactions.