To effectively implement the FATF’s risk-based approach (RBA) for AML/CFT, financial institutions should collect and monitor specific data points that enable accurate risk assessment and mitigation. Here are some of the most critical data points:

**1. Customer Identification Data**

* **Personal Information**: Full name, date of birth, nationality, and residence details.
* **Business Information (for corporate clients)**: Registered name, business type, country of incorporation, and ownership structure.
* **Beneficial Ownership**: Identifying individuals with significant control over the entity.
* **Politically Exposed Person (PEP) Status**: PEP classification of customers and their immediate family or associates.

**2. Geographic and Country Data**

* **Country of Residence or Operation**: Key for assessing country-specific risks based on FATF lists and other AML/CFT guidance.
* **Geographic Locations of Transactions**: Identifying cross-border transactions, especially with high-risk jurisdictions.
* **Country Risk Rating**: Informed by sanctions lists, corruption indices, and AML/CFT regulations.

**3. Transactional Data**

* **Transaction Volume and Frequency**: Patterns and trends that could indicate abnormal activity.
* **Transaction Types**: Cash deposits, international wire transfers, high-value transactions, or unusual transaction methods.
* **Transaction Amounts**: Especially significant amounts inconsistent with the customer's profile or business type.
* **Destination and Source of Funds**: Countries, individuals, or institutions involved in transactions, particularly if located in or linked to high-risk regions.

**4. Customer Profile and Behavior**

* **Customer Type**: Categorizing customers by risk type (e.g., high-cash businesses, non-profit organizations, individual vs. corporate).
* **Account Activity Patterns**: Normal vs. abnormal transaction patterns for the customer’s profile.
* **Changes in Behavior**: Sudden increases in transaction volume, changes in geographical transaction patterns, or new, unexplained account activities.

**5. Product and Service Data**

* **Type of Product or Service Used**: Identifying high-risk services (e.g., private banking, correspondent banking, high-value commodities trading).
* **Method of Delivery**: Channels through which products/services are delivered (e.g., online banking, non-face-to-face interactions, third-party intermediaries).
* **Anonymity of Products**: Services that provide anonymity, such as stored value cards, are higher risk and require additional monitoring.

**6. Risk Assessment and Monitoring Data**

* **Customer Risk Score**: A calculated risk score based on factors such as customer type, geographic location, and transaction history.
* **Enhanced Due Diligence (EDD) Triggers**: Flags for when a customer requires EDD, such as transactions with high-risk countries, unusual patterns, or PEP status.
* **Monitoring Thresholds**: Set thresholds for transaction alerts or reviews, which can be adjusted based on evolving risk levels.
* **Suspicious Activity Reports (SARs)**: Records of SAR filings, reasons for suspicion, and resolution status.

**7. Internal Compliance and Control Data**

* **Training Records**: Tracking AML/CFT training participation by employees.
* **Audit Logs and Review Findings**: Results of internal audits, third-party reviews, or compliance checks.
* **System and Process Changes**: Updates to thresholds, controls, and procedures based on recent findings or changes in regulatory guidance.

By focusing on these data points, financial institutions can achieve a well-rounded understanding of ML/TF risks, align with FATF's guidelines, and enhance the effectiveness of their risk-based AML/CFT programs.