Version 2.0

Anti-Money Laundering (AML) Monitoring Compliance Guidance

This document presents a framework for monitoring compliance with Anti-Money Laundering (AML) regulations using Jube, an open-source fraud prevention and transaction monitoring tool. The framework aligns with guidance from the Financial Action Task Force (FATF) and the Wolfsberg Principles.

JUBE

JUBE

Amendments

Date	Author	Version	Description
28th February 2025	Richard Churchman	2.0	Substantial update and rewrite from version one. Improved writing and linked to documentation instead of using images.

JUBE

Introduction to Methodology

This document outlines a framework designed to assist in monitoring compliance with Anti-Money Laundering (AML) regulations using **Jube**, open-source software utilized for fraud prevention and transaction monitoring, but with a sharp focus on regulatory prescribed transaction monitoring such as Anti Money Laundering (AML). This framework is based on regulatory guidance from the **Financial Action Task Force (FATF)**, and the **Wolfsberg Principles**. Jube, being open-source and with global reach, is foreseeably exposed to local market regulations, and the working assumption is that such regulations will be derivative of FATA and the Wolfsberg Principles to some extent, but not enough to be compliant.

The scope of AML compliance is extensive, and this document focuses specifically on the **monitoring requirements** outlined in the guidance. While guidance does not endorse a rigid, unthinking approach, it highlights several clear risk factors, including:

- **Country and Geographic Risk**
- **Distribution Channels Risk**
- **Transaction Behavioural Risk**
- **Product Liquidity and Use of Cash-Like Instruments** (e.g., utility instruments like petrol, highly negotiable instruments like Bitcoin, and products linked to crime such as gambling and adult services)
- **Anonymous Financial Products**
- **Online Products Vulnerable to Impersonation**
- **Person-to-Person Remittance and Low Financial Inclusion Products**

The guidance acknowledges that risk factors often interact, with high-risk factors potentially being offset by low-risk ones. While the guidance suggests a subjective, experience-based weighting of risks, this approach is prone to judgmental bias. A **data-driven approach**, combined with subjective judgment, is recommended as a more reliable method. This trade-off approach aligns well with **supervised and unsupervised learning techniques**.

Core Principles of AML Monitoring

The overarching principle of AML compliance is **Know Your Customer (KYC)**, achieved through due diligence, understanding the business and products, and conducting ongoing transaction monitoring in a timely (though not necessarily real-time) manner. Financial institutions are granted significant latitude under a **Risk-Based Approach (RBA)**, allowing them to assess risk factors and implement controls proportionate to the risks posed by their products.

Countermeasures and Customer Due Diligence (CDD)

The primary countermeasure available to financial institutions is the rigorous application of **Customer Due Diligence (CDD)**. CDD aims to ensure that institutions can verify the identity of customers, beneficial owners, and the nature of their transactions. There are five practical levels of CDD:

1. **Anonymous**: No due diligence.

2. **Simplified Due Diligence (SDD)**: Verification of identity, sanctions, political exposure, and address. Monitoring product use within strict thresholds and limits.
3. **Enhanced Due Diligence (EDD)**: Verification of identity, address, and source of funds.
4. **Enhanced Monitoring (EM)**: Diligent monitoring of transactions within tight thresholds or manually.
5. **Suspicious Activity Reporting (SAR)**: Reporting suspicious activities to financial crime investigation authorities.

The weaker the CDD, the greater the exposure to money laundering. Therefore, the standard of CDD must be considered during monitoring, alongside a thorough understanding of product risks and prevailing risk factors. Additionally, maintaining a robust **audit trail** is critical to demonstrate diligent transaction monitoring and CDD escalation to regulators.

Automated Monitoring Systems

The use of **automated monitoring systems** is permitted and, in some cases, encouraged by regulatory guidance. However, the Money Laundering Reporting Officer (MLRO) must fully understand how these systems function. Given the evolving nature of financial crime, monitoring frameworks must be adaptable to emerging threats.

Regarding **"tipping off"** (the risk of alerting suspects to investigations), there is no requirement for real-time monitoring. Implementing systems on a **batch or asynchronous basis** (after the event) can reduce the risk of compromising investigations. Notwithstanding, Jube is real-time in its nature, refereeing to data integration as follows in this document.

Jube's Data-Driven Risk-Based Approach

Jube promotes a **Data-Driven Risk-Based Approach** to monitoring, addressing a key challenge in AML: the absence of absolute outcomes. Instead, AML outcomes involve varying levels of suspicion. To address this, the proposed model focuses on **anomaly detection** and **classification based on subjective levels of suspicion**, as determined by rules that escalate cases to case management.

This approach ensures that monitoring is both **adaptive** and **proportionate**, leveraging data-driven insights to enhance the effectiveness of AML compliance efforts.

JUBE

About Jube

Jube is an **open-source software** designed for monitoring transactions and events. It features:

- **Real-Time Data Processing**
- **AI-Driven Decision-Making**
- **Case Management**

Jube excels in **fraud prevention** and **abuse detection**, with a particular focus on the **Anti-Money Laundering (AML) transaction monitoring** use case. The platform is built on the principle that adjacent use cases—while keeping in mind Jube's fastidious real-time capabilities—will derive from the same foundational methodology.

Focus on AML Transaction Monitoring

Jube maintains a sharp focus on the **AML transaction monitoring** use case, developing deep expertise in this area. The platform's training and support are strongly oriented toward this use case and its associated methodology.

Value Proposition for End Users

It is recognized that the discipline of AML is well-established. When end users evaluate Jube, they are typically not looking for a greenfield implementation but rather:

1. **Cost Reduction:** Eliminate the prohibitive costs associated with proprietary solutions.
2. **Vendor Lock-In Eradication:** Gain flexibility and control by avoiding dependency on single vendors.
3. **Improved Compliance:** Access more advanced tooling to enhance compliance with regulatory requirements.

Jube represents a powerful, cost-effective, and flexible solution for AML transaction monitoring. By leveraging its real-time capabilities, advanced tooling, and open-source nature, financial institutions can reduce costs, eliminate vendor lock-in, and enhance compliance. Jube's focus on AML, combined with its adaptability to derivative use cases, makes it an asset in the fight against financial crime.

Key Notes

1. **Real-Time Capabilities:** Jube's real-time processing ensures timely detection and response to suspicious activities, a critical requirement for AML compliance.
2. **Open-Source Advantage:** As an open-source platform, Jube offers transparency, customization, and cost efficiency, making it an attractive alternative to proprietary solutions.
3. **Derivative Use Cases:** While AML is the primary focus, Jube's methodology can be extended to other use cases, such as fraud detection and cybersecurity.
4. **Advanced Tooling:** Jube provides access to innovative AI and analytics tools, enabling users to stay ahead of evolving financial crime trends.

5. **Regulatory Alignment:** The platform is designed to help institutions meet and exceed regulatory requirements, reducing the risk of non-compliance.

Further Reading

- **About Jube:** https://jube-home.github.io/jube/
- **Getting Started:** https://jube-home.github.io/jube/GettingStarted/
- **GitHub:** https://github.com/jube-home/jube

Risk Factors

Risk factors are developed by aggregating customer account transactions and product characteristics. These factors focus on **four core areas**, aligned with the most prevalent risk factors outlined in regulatory guidance:

Characteristic Grouping	Description
Product	This grouping captures the behavioural characteristics of financial products. It includes summary statistics that describe typical product behaviour and the degree of variation in that behaviour.
Product MCC Spend	This grouping contains aggregated data on spending by **Merchant Category Code (MCC)** for a given product type. It provides summary statistics describing typical monetary outflows for the product.
Product Country Spend	This grouping contains aggregated data on spending by **Country Code** for a given product type. It provides summary statistics describing typical monetary outflows for the product.
Account Characteristics	This grouping captures behavioural characteristics of individual accounts. It includes summary statistics and behavioural flags that describe account behaviour and the operating environment of the account.

Modelling Risk Factors in Jube

The following factors will be modelled in **Jube** to enable **Machine Learning** and **Activation Rules**. In Jube, risk factors can be modelled using **Abstraction Rules**. Below is an explanation of the factors within their core groupings:

Sanctions

- **Distance:** First and foremost, the obligation to screen customer names, source and destination account names via sanctions lists. Distance algorithms ensure than minor variations, deliberate or otherwise, do not evade sanctions screening.

Product Characteristics

- **Typical Behaviour**: Summary statistics describing the normal usage patterns of the product (e.g., average transaction size, frequency, and volume).
- **Behavioural Variance**: Measures of how much the product's usage deviates from the norm (e.g., standard deviation of transaction amounts or frequencies).

Product MCC Spend

- **MCC-Based Spending Patterns**: Aggregated data on spending by **Merchant Category Code (MCC)**, such as retail, travel, or entertainment.
- **Typical Outflows**: Summary statistics describing the average monetary outflows for specific MCCs associated with the product.

Product Country Spend

- **Country-Based Spending Patterns**: Aggregated data on spending by **Country Code**, highlighting geographic trends in product usage.
- **Typical Outflows**: Summary statistics describing the average monetary outflows for specific countries associated with the product.

Account Characteristics

- **Behavioural Flags**: Indicators of unusual account activity (e.g., sudden spikes in transaction volume, changes in spending patterns).
- **Environmental Factors**: Contextual information about the account's operating environment (e.g., high-risk jurisdictions, use of anonymous products).
- **Summary Statistics**: Metrics describing the account's transaction behaviour (e.g., average balance, transaction frequency, and amounts).

By modelling these risk factors, Jube enables a **data-driven approach** to AML monitoring, allowing financial institutions to identify anomalies, assess risks, and implement targeted controls effectively. This structured approach ensures compliance with regulatory requirements while minimizing judgmental bias and enhancing the overall effectiveness of transaction monitoring.

Lists

The **Data-Driven Risk-Based Approach** relies on several lists that can be referenced in **Activation Rules** and **Machine Learning** models. These lists require regular maintenance to remain effective. Below are the key lists that should be included and regularly updated by the MLRO:

List Name	Description
FATF Uncooperative Countries	A list of countries identified by the **Financial Action Task Force (FATF/GAFI)** as non-cooperative in AML efforts.
High-Risk Human Trafficking Countries	A list of countries identified as high-risk for human trafficking, based on resources such as the **UNODC Global Report on Trafficking in Persons**.
Low GDP Per Capita Countries	A list of countries with low GDP per capita, used to identify high spending from regions with limited economic means.
Political Instability Countries	A regularly updated list of countries exhibiting political instability risks.
Sanctioned Countries	A list of countries subjected to international sanctions.

Key Notes

- **Dynamic Updates**: These lists must be regularly maintained to reflect current global risks and regulatory changes.

- **Integration with Rules**: The lists are integrated into **Activation Rules** and **Machine Learning** models to enhance risk detection and monitoring.
- **Proactive Risk Management**: By leveraging these lists, financial institutions can proactively identify and mitigate risks associated with specific countries or regions.

Further Reading

- **Lists:** https://jube-home.github.io/jube/Configuration/Models/Lists/
- **Dictionaries:** https://jube-home.github.io/jube/Configuration/Models/Dictionaries/

Sanctions

The primary requirement is to screen customer names, as well as the names of source and destination accounts, against sanctions lists. To account for minor variations—whether intentional or unintentional—distance algorithms (e.g., Levenshtein Distance) are used to ensure effective screening.

Characteristic	Definition	Period Grouping
Sanctions Distance Recipient on Send	A sanctions match with a Levenshtein Distance greater than two, applied to the recipient's name for each transaction.	**Period:** For each transaction
Sanctions Distance Sender on Receipt	A sanctions match with a Levenshtein Distance greater than two, applied to the sender's name for each transaction.	**Period:** For each transaction

Sanctions could be taken to be any textual dataset that has been published via a regulator or central bank, such as US Office of Foreign Assets Control, or more universally available as CSV from consolidated sources such as OpenSanctions.

Key Notes

1. **Assumption:** Sanctions checks are performed during customer onboarding. Therefore, controls are focused solely on monitoring inflows and outflows.
2. **Levenshtein Distance:** This algorithm measures the difference between two strings (e.g., names) by calculating the number of edits (insertions, deletions, or substitutions) required to make them match. A distance greater than two indicates a potential match despite minor variations.
3. **Purpose of Screening:** Ensures compliance with sanctions regulations by identifying and flagging high-risk transactions or entities.

Further Reading

- **Sanctions:** https://jube-home.github.io/jube/Configuration/Sanctions/

JUBE

Product Characteristics

These characteristics are available for each **Product ID** and are used to describe the typical behaviour and variability of financial products. Below is a detailed breakdown of each characteristic, including its definition, applicable periods, and grouping:

Characteristic	Definition	Period Grouping
Average Inflow	The average amount deposited into a product.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Variance Inflow	Describes the variability of the average inflow, indicating its reliability.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Average Outflow	The average amount withdrawn from a product.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Variance Outflow	Describes the variability of the average outflow, indicating its reliability.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Average Maximum Inflow	The average of the maximum deposit amounts across accounts for the product.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Variance Maximum Inflow	Describes the variability of the average maximum inflow, indicating its reliability.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Average Maximum Outflow	The average of the maximum withdrawal amounts across accounts for the product.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Variance Maximum Outflow	Describes the variability of the average maximum outflow, indicating its reliability.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Average Minimum Inflow	The average of the minimum deposit amounts across accounts for the product.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Variance Minimum Inflow	Describes the variability of the average minimum inflow, indicating its reliability.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Average Minimum Outflow	The average of the minimum withdrawal amounts across accounts for the product.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.

Characteristic	Definition	Period Grouping
Variance Minimum Outflow	Describes the variability of the average minimum outflow, indicating its reliability.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Average Frequency Inflow	The average frequency (count) of deposits across accounts for the product.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Variance Frequency Inflow	Describes the variability of the average frequency of inflows, indicating its reliability.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Average Frequency Outflow	The average frequency (count) of withdrawals across accounts for the product.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Variance Frequency Outflow	Describes the variability of the average frequency of outflows, indicating its reliability.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.

Key Notes

- **Periods**: Metrics are calculated over daily, weekly, monthly, yearly, and lifetime periods to provide a comprehensive view of product behaviour.
- **Grouping**: Data is grouped by **Point of Sale (POS)** and **Cash/Quasi-Cash** transactions to ensure granularity and relevance.
- **Variance Metrics**: These values indicate the reliability of the average metrics by measuring the degree of variability in the data.

These characteristics enable a detailed understanding of product behaviour, supporting effective monitoring, anomaly detection, and risk assessment in AML compliance efforts.

Further Reading:

- **Abstraction Rules:** https://jube-home.github.io/jube/Configuration/Models/AbstractionRules/
- **TTL Counters:** https://jube-home.github.io/jube/Configuration/Models/TTLCounters/
- **Environment Variables:** https://jube-home.github.io/jube/Concepts/EnvironmentVariables/

Product MCC Spend

These characteristics are available for each **Product ID** and **Merchant Category Code (MCC)**, providing insights into spending patterns associated with specific product types and merchant categories. Below is a detailed breakdown of each characteristic, including its definition, applicable periods, and grouping:

Characteristic	Definition	Period Grouping
Average Transaction Amount	The average transaction amount for a given product and MCC.	**Periods**: Rolling Three Months.
Variance Transaction Amount	Describes the variability of the average transaction amount, indicating its reliability.	**Periods**: Rolling Three Months.

Key Notes

- **Periods**: Metrics are calculated over a **rolling three-month period** to provide a dynamic and up-to-date view of spending behaviour.
- **Focus**: These metrics help identify typical spending patterns and anomalies for specific product and MCC combinations, supporting targeted monitoring and risk assessment.

These characteristics enable financial institutions to better understand and monitor transaction behaviour, enhancing their ability to detect unusual activity and comply with AML regulations.

Product Country Spend

These characteristics are available for each **Product ID** and **Country Code of Spend**, providing insights into spending patterns associated with specific product types and geographic regions. Below is a detailed breakdown of each characteristic, including its definition, applicable periods, and grouping:

Characteristic	Definition	Period Grouping
Average Transaction Amount	The average transaction amount for a given product and country.	**Periods**: Rolling Three Months.
Variance Transaction Amount	Describes the variability of the average transaction amount, indicating its reliability.	**Periods**: Rolling Three Months.

Key Notes

- **Product Country Spend**: Focuses on geographic spending patterns, helping identify unusual activity in specific regions.

CDD and Account Factors

These characteristics are available for each **Account or Relationship ID**, providing detailed insights into customer behaviour and due diligence status. Below is a detailed breakdown of each characteristic, including its definition, applicable periods, and grouping:

Characteristic	Definition	Period Grouping
eKYC Flag	A Yes/No (1/0) flag indicating if the customer has been verified by **eKYC verification methods**.	**Periods**: Lifetime.

Characteristic	Definition	Period Grouping
Manual KYC Flag	A Yes/No (1/0) flag indicating if the customer has been verified by **manual KYC verification methods**.	**Periods**: Lifetime.
Days Since Account Open	The number of days elapsed since the account was opened.	**Periods**: Lifetime.
Days Since Account Transacting	The number of days elapsed since the account first started transacting.	**Periods**: Lifetime.
Identity Duplication	A Yes/No (1/0) flag indicating if heuristics (e.g., name, address, date of birth, email, or device recognition) suggest duplication with another account.	**Periods**: Lifetime.
Inflow	The absolute amount deposited into the customer account.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Outflow	The absolute amount withdrawn from the customer account.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Maximum Transaction Inflow	The largest deposit into the customer account.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Minimum Transaction Inflow	The smallest deposit into the customer account.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Maximum Transaction Outflow	The largest withdrawal from the customer account.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Minimum Transaction Outflow	The smallest withdrawal from the customer account.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Transaction Frequency Inflow	The number of deposits into the customer account.	**Periods**: Day, Week, Month, Year,

Characteristic	Definition	Period Grouping
		Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Transaction Frequency Outflow	The number of withdrawals from the customer account.	**Periods**: Day, Week, Month, Year, Lifetime. **Grouped**: POS and Cash/Quasi Cash.
Source of Funds Underwritten	A Yes/No value indicating if a **Source of Funds Underwriting Process** has been completed.	**Periods**: Lifetime.
Spends Outside Top 10 MCC	Indicates if the customer spends outside the **Top 10 Merchant Category Codes (MCCs)** for the product.	**Periods**: Day, Week, Month, Year, Lifetime.
Spends Outside Top 5 Countries	Indicates if the customer spends outside the **Top 5 Countries** for the product.	**Periods**: Day, Week, Month, Year, Lifetime.
Spends Outlier for MCC	Indicates if the customer's spending falls outside the range of 90% of customers for a given MCC.	**Periods**: Day, Week, Month, Year, Lifetime.
Spends Outlier for Country	Indicates if the customer's spending falls outside the range of 90% of customers for a given country.	**Periods**: Day, Week, Month, Year, Lifetime.

Key Notes

- **CDD and Account Factors**: Provides a comprehensive view of customer behaviour, due diligence status, and transaction patterns, enabling effective monitoring and risk assessment.
- **Grouping**: Transaction data is grouped by **Point of Sale (POS)** and **Cash/Quasi-Cash** to ensure granularity and relevance.
- **Periods**: Metrics are calculated over daily, weekly, monthly, yearly, and lifetime periods, as well as rolling three-month periods for dynamic insights.

These characteristics support a **data-driven approach** to AML compliance, enabling financial institutions to detect anomalies, assess risks, and implement targeted controls effectively.

Data Integration

The effectiveness of risk factors in Jube relies on the seamless integration of relevant data sources. Integration is achieved through the concept of **models**, which are configured to process, aggregate, and analyse data for monitoring purposes. Below is an outline of the proposed models, integration methods, and additional functionalities:

Example Models

The following models are recommended to ensure comprehensive data integration:

1. **Payment scheme authorisations**
    - **Purpose:** Capture all authorization records for payment scheme or brand transactions.
    - **Outcome:** Provides a complete and enhanced view of transactions processed through these payment networks.
2. **Financial Transactions and Clearing**
    - **Purpose:** Capture all financial transactions representing inflows and outflows to an account.
    - **Includes:** Deposits, withdrawals, and abridged cleared payment scheme transactions.
3. **Customer Due Diligence (CDD) Events**
    - **Purpose:** Capture events related to customer verification processes.
    - **Examples:** Address validation, identity validation, source of funds verification, sanctions matching, etc.

Model Configuration

Each model is configured via Jube's user interface, where key values and fields are specified. The **Request XPath** page is used to define:

- **Additional Fields:** Fields made available for rule creation.
- **Search Keys:** Designated fields that enable the model to perform aggregations as outlined in the risk factors section.

Integration Method

The proposed integration method involves the following steps:

1. **Real-Time or Batch Preparation:** Prepare messages in real-time or relay data from a database or other latent data store.
2. **Message Compilation:** Compile the data into a JSON message.
3. **Data Transmission:** Relay the message to Jube via HTTP.
4. **Serial Processing:** Even if the data is latent, it will be processed serially in ascending datetime order, simulating real-time transaction processing.

Optional IP Address Decoding

Where available, IP addresses are decoded to provide geographic and contextual information about the session. This is achieved using an **Inline Script** to call **IP2Location**, which returns details such as:

- Country
- Coordinates
- ISP (Internet Service Provider)
- Region
- Usage Type/Connection
- Net Speed
- City
- Domain
- IDD & Area Code
- ZIP Code
- Elevation
- Weather Station

Outcomes of Integration

The integrated data and risk factors can be utilized in the following ways:

- **Comprehensive Data Coverage:** Ensures all relevant transaction and customer data is captured and analysed.
- **Enhanced Monitoring:** Enables real-time or near-real-time processing of latent data.
- **Geographic Insights:** Decodes IP addresses to provide contextual information for risk assessment.
- **Flexibility:** Supports integration with external services for PEP and sanctions validation.
- **Actionable Insights:** Facilitates the creation of dashboards, machine learning models, and activation rules for proactive AML compliance.

Key Notes

1. **Latent Data Processing:** Even when data is not real-time, Jube processes it serially in ascending datetime order to simulate real-time transaction processing.
2. **IP2Location Integration:** The use of IP2Location provides granular geographic and contextual insights, enhancing risk assessment capabilities.
3. **Regulatory Compliance:** The integration of these models ensures compliance with AML (Anti-Money Laundering) and regulatory requirements.

4. **Scalability:** The proposed models and integration methods are designed to scale with increasing transaction volumes and data complexity.
5. **Customization:** Jube's user interface allows for flexible configuration of models, enabling institutions to tailor the system to their specific needs.

Further Reading

- Models: https://jube-home.github.io/jube/Configuration/Models/Models/
- Request XPath: https://jube-home.github.io/jube/Configuration/Models/RequestXPath/
- Inline Scripts: https://jube-home.github.io/jube/Configuration/Models/InlineScripts/
- Gateway Rules: https://jube-home.github.io/jube/Configuration/Models/GatewayRules/

MLRO Dashboards

The framework outlined in this document emphasizes that AML (Anti-Money Laundering) monitoring must be an evolving process. To support this, it is critical that **MLRO Dashboards** provide timely, comprehensible, and visually intuitive reporting. These dashboards enable the **Money Laundering Reporting Officer (MLRO)** to gain a deep understanding of:

- **Product Behaviour**
- **Customer Activity**
- **Territorial Risks**
- **Distribution Channels**

The scope of MLRO reports should not be limited to the current framework but should also serve as a tool for proactively creating new controls and adapting to emerging risks.

Objectives of MLRO Dashboards

The primary objectives of MLRO dashboards are:

1. **Drive Innovation:** Facilitate the creation of innovative control hypotheses to address emerging risks.
2. **Monitor Rule Performance:** Profile the performance of rules and assess their proportional contribution to the Data-Driven Risk-Based Approach.
3. **Evolve Risk Factors:** Ensure that risk factors and rules are continuously updated based on insights derived from the dashboard.

Design and Customization

MLRO Dashboards can be instantly designed and customized using **Jube's Reporting Designer**. This tool allows for the creation of tailored visualizations and reports that align with the MLRO's specific needs, ensuring flexibility and adaptability.

Benefits of MLRO Dashboards and Risk Factor Lists

The combination of MLRO Dashboards and Risk Factor Lists ensures that financial institutions can:

- **Monitor and Adapt:** Continuously evolve their AML monitoring frameworks based on real-time insights.
- **Proactively Manage Risks:** Identify emerging threats and implement targeted controls to mitigate them.
- **Ensure Compliance:** Maintain alignment with regulatory requirements and global best practices.

Key Notes

1. **Proactive Risk Management:** MLRO Dashboards are not just reactive tools but also enable proactive risk management by identifying trends and anomalies early.

2. **Customizable Reporting:** Jube's Reporting Designer allows MLROs to create dashboards tailored to their institution's unique risk profile and regulatory needs.
3. **Data-Driven Insights:** The dashboards leverage data-driven insights to ensure that risk factors and rules remain relevant and effective.
4. **Regulatory Alignment:** By providing comprehensive and timely reporting, MLRO Dashboards help institutions stay compliant with evolving AML regulations.
5. **Scalability:** The framework is designed to scale with growing transaction volumes and increasing complexity in financial crime patterns.

Further Reading

- **Visualisations:** https://jube-home.github.io/jube/Configuration/Visualisations/

Machine Learning

Jube supports the use of **risk factors** in both **Machine Learning (ML)** and **Activation Rules**. The platform offers two types of Machine Learning:

1. **Classification (Supervised Learning)**
2. **Unsupervised Learning**

Classification (Supervised Learning)

- **Purpose:** Identifies accounts that conform to a known classification, such as "Suspected Money Laundering."
- **Process:** Analysts must diligently flag highly suspicious transactions in the **Case Management System** using the star rating functionality.
- **Outcome:** A curated sample of highly suspicious transactions is used to train Jube's embedded classification engine.
- **Goal:** Distils numerous risk factors into a **score** that indicates the likelihood of a transaction being related to money laundering.
- **Use Case:** The score is recalled for each transaction processed through Jube and can be used in **Activation Rules** to escalate accounts to **Case Management** if the score exceeds a predefined threshold.

Limitations of Classification:

1. **Rapidly Changing Risks:** Classification models are less effective in environments where risk typologies evolve quickly, as they are better at detecting known patterns than emerging risks.
2. **Anomaly Detection:** Classification models are less capable of identifying new or anomalous behaviour.

Unsupervised Learning

To counter the limitations of Classification, Jube employs **One-Class Support Vector Machine (SVM)**, a technique that groups customers based on similar behaviours using the risk factors described in this document. Unlike Classification, Unsupervised Learning does not require transactions to be marked as suspicious to learn.

Benefits of Unsupervised Learning:

1. **Anomaly Detection:**
    - Most customers fall into a small number of clusters representing typical behaviour.
    - Outlier clusters represent anomalous behaviour, which can be flagged for further investigation.
2. **Unbiased:**

- Anomalies are identified based on behavioural similarities without predefined labels.

Exhaustive Adaptation Concepts

Traditional risk management or anomaly detection is typically rule-based. Examples of rules might include:

- More than four transactions in one day.
- More than two declined transactions in one day.
- More than two different transactions in one day.
- More than five transactions at the same merchant in one day.
- Transactions more than twice (x2) the customer's average transaction.

While rules are effective, their derivation is often anecdotal, and thresholds are rarely adapted over time. This leads to:

- **Rule Proliferation:** The number of rules tends to grow, making them difficult to manage.
- **Diminishing Efficacy:** Rules often fail to adapt to new risk typologies, reducing their effectiveness.

Jube combines **Supervised** and **Unsupervised Learning** to create a robust and adaptive risk management system.

Key Steps in Jube's Machine Learning Process:

1. **Data Extraction:** Data is extracted from Jube for **Abstraction Rules**, which include continuous values such as transaction counts, declined transactions, and customer averages.
2. **Anomaly Detection:** Data is trained based on anomaly, where highly anomalous events are classified as fraudulent.
3. **Blending Feedback Data:** Anomaly data is blended with specific feedback data tagged by analysts, which is lower in volume but highly salient.
4. **Neural Network Training:** Multiple neural network topologies (e.g., hidden layers, activation functions) are trialled, evolved, and trained based on the data.

Outcome:

- A **complex neural network model** is created on a quantitative basis.
- The model identifies optimal topology using the **Levenberg-Marquardt Backpropagation Algorithm**.
- The system continuously adapts by retraining models in a **champion-challenger framework**, ensuring ongoing relevance and accuracy.

Exhaustive Training Algorithm

Jube's exhaustive training algorithm follows these steps:

1. **Variable Collation:** Eligible variables (e.g., from Abstraction Calculations, TTL Counters, and Abstraction Rules) are collated.
2. **Data Sampling:** A sample of data is extracted from the archive, excluding class variables.
3. **Statistical Analysis:** Statistics are performed on the sample for Z-score normalization.
4. **Normalization:** Continuous variables are normalized, while binary variables remain unchanged.
5. **Anomaly Detection:** A **One-Class Support Vector Machine** is trained to detect anomalies.
6. **Data Blending:** Anomaly data is blended with feedback data tagged by analysts.
7. **Model Training:** Neural networks are trained exhaustively, with topology and variables selected randomly.
8. **Performance Validation:** Models are validated using testing data, and the most performant model is selected.
9. **Monte Carlo Simulation:** A Monte Carlo simulation is performed to analyse model sensitivity.

Key Notes

1. **Adaptability:** Jube's models are continuously updated to adapt to new data and emerging risks.
2. **Anomaly Detection:** Unsupervised Learning ensures that unknown or emerging risks are identified.
3. **Efficiency:** The exhaustive training algorithm optimizes model topology, reducing training time and improving generalization.
4. **Real-Time Processing:** Scores generated by ML models can be used in real-time to decline transactions or escalate cases.
5. **Transparency:** All training steps and model performance metrics are stored in the database for future analysis and improvement.

Further reading

- **Exhaustive Adaptation:** https://jube-home.github.io/jube/Configuration/ExhaustiveAdaptation/
- **HTTP Adaptation:** https://jube-home.github.io/jube/Configuration/Models/HTTPAdaptation/Index.html

JUBE

Activation Rules

Activation Rules are used to escalate accounts and transactions into **Case Management** based on risk factors and machine learning outcomes. Below is a list of proposed Activation Rules:

Name	Description
High TXN Amount >= 4000	A transaction exceeds EUR 4000 in value.
Automated Fuel Dispenser (5542) >= 3txns in 1 day	More than three fuel dispensers used in a single day. (Applies to utility transactions.)
High Velocity >= 7 Txns in a day	More than seven transactions in a day.
High Risk MCC >= 4txns in 5 hours	More than four transactions in a high-risk MCC within five hours.
High Withdrawal >= 2000 in 2 days	More than 2000 EUR withdrawn from an account within two days.
High Risk MCC High Amount >= 1000 in 2 days	Transactions in high-risk MCCs (e.g., utilities or negotiable instruments) exceeding 1000 EUR in two days.
High Risk Country >= 2000 in 5 hours	More than 2000 EUR transacted in a high-risk country within five hours.
High Amount >= 3000 over 2 days	More than 3000 EUR transacted within two days.
3 Countries in 6 hours and 1 HR Country	More than three transactions in three different countries within six hours, with one high-risk country.
3 Countries in 1 day Not Ecommerce	More than three transactions in one day, excluding eCommerce transactions.
High Risk MCC >= 4 Txns in 6 hours	More than four transactions in high-risk MCCs within six hours.
Same Merchant >=3 txns in 1 day	Transactions where the same merchant is used more than three times in one day.
ATM >= 500.00 EUR/day on 3 consecutive days	ATM withdrawals exceeding 500 EUR per day for three consecutive days.
High Risk MCC >= 50,000 in 1 day	A high-risk MCC transaction exceeding EUR 50,000 in one day.
High Deposit >= €300 in 6 hours	More than 300 EUR deposited into an account within six hours.
Load then Refund in 1 day	A load followed by a refund observed within one day.

Name	Description
Refund on two consecutive days	Two refunds observed on two consecutive days.
Multiple Refunds >= 3 in 2 days	More than three refunds made within two days.

Key Notes

- **Classification**: Focuses on known patterns and generates a risk score for transactions.
- **Clustering**: Identifies new and anomalous behaviour by grouping similar accounts.
- **Activation Rules**: Escalate cases to Case Management based on predefined thresholds and risk factors.
- By combining **Classification**, **Clustering**, and **Activation Rules**, Jube provides a comprehensive framework for detecting and managing AML risks, ensuring compliance with regulatory requirements, and adapting to emerging threats.

Further Reading

- **Basic Activation Rules:** https://jube-home.github.io/jube/Configuration/Models/BasicActivationRules/
- **Response Elevation:** https://jube-home.github.io/jube/Configuration/Models/ResponseElevation/
- **TTL Counter Activation Rule Incrementation:** https://jube-home.github.io/jube/Configuration/Models/TTLCounterActivationRuleIncrementation/
- **Activation Watcher:** https://jube-home.github.io/jube/Configuration/Models/ActivationWatcher/
- **Activation Rule Notifications:** https://jube-home.github.io/jube/Configuration/Models/ActivationRuleNotifications/
- **Activation Rules Suppression:** https://jube-home.github.io/jube/Configuration/Models/ActivationRulesSuppression/
- **Rule Compilation Algorithm:** https://jube-home.github.io/jube/Configuration/Models/RuleCompilationAlgorithm/
- **Reprocessing:** https://jube-home.github.io/jube/Configuration/Reprocessing/

Case Management

Case Management is the central hub where accounts flagged by rules are reviewed and investigated by analysts. In Jube, cases are organized by **workstreams**, and each case can have one of the following statuses:

- **Refer to MLRO**: Escalated to the Money Laundering Reporting Officer for further review.
- **No Further Action**: No suspicious activity detected; case closed.
- **Pending EDD Documentation**: Awaiting Enhanced Due Diligence (EDD) documentation.
- **Pending CDD Documentation**: Awaiting Customer Due Diligence (CDD) documentation.
- **SAR Sent by MLRO**: A Suspicious Activity Report (SAR) has been filed by the MLRO.

Case Audit

Jube provides robust **Case Audit** features to ensure transparency and compliance. These features allow regulators to review the lifecycle of a case on demand. Key audit functionalities include:

1. **Single Open Case per Account**:
    - Only one case can be open for an account at any given time.
    - Once a case is closed, it can be reopened if necessary.
2. **Full Case Journal**:
    - A complete record of all open and previously closed cases is maintained.
3. **Action Tracking**:
    - Every action performed on a case—whether voluntary (e.g., adding notes) or involuntary (e.g., reviewing a case)—is recorded in the audit trail.
4. **Analyst Notes**:
    - Analysts are required to add notes to explain the circumstances surrounding case creation and their actions during the investigation.

Case Uploads

As part of the investigation process, **Enhanced Due Diligence (EDD)** documentation may be required. Jube allows for the seamless upload and management of such documents:

- **Document Upload**: EDD documentation can be uploaded directly to the case.
- **Centralized Access**: All relevant documents are stored in a specific location for easy review.

Case Escalation

Cases may need to be escalated for further review by the MLRO or for the creation of a **Suspicious Activity Report (SAR)**. Escalation in Jube is straightforward:

1. **Change Workflow Status**:
    - Analysts can escalate a case by changing its workflow status to **"Refer to MLRO"**.
2. **MLRO Review**:
    - The MLRO can filter and view escalated cases for review.
3. **SAR Creation**:
    - SARs can be created by completing a case form within Jube.
    - MLRO reports allow for the creation of **template SARs**, which can be emailed directly to the relevant authorities.

Key Notes

- **Organized Workstreams**: Cases are categorized and managed efficiently.
- **Comprehensive Audit Trail**: Ensures transparency and regulatory compliance.
- **Document Management**: Centralized storage and access to EDD documentation.
- **Seamless Escalation**: Easy escalation to MLRO and SAR creation.
- **Analyst Accountability**: Mandatory notes, and action tracking ensure thorough investigations.

By leveraging Jube's Case Management capabilities, financial institutions can effectively investigate and resolve flagged cases, maintain compliance with regulatory requirements, and ensure a robust AML monitoring framework.

Further Reading

- **Case Management:** https://jube-home.github.io/jube/Configuration/CaseManagement/

Summary

This document presented a framework for monitoring Anti-Money Laundering (AML) compliance using **Jube**, an open-source software designed for fraud prevention and transaction monitoring. The framework is based on regulatory guidance from the **Financial Action Task Force (FATF)** and the **Wolfsberg Principles**, focusing on transaction monitoring and risk-based approaches to AML compliance.

Key Focus Areas:

1. **Risk Factors**:
    - **Country and Geographic Risk**: High-risk jurisdictions.
    - **Transaction Behavioural Risk**: Unusual transaction patterns.
    - **Product Risk**: Liquidity, cash-like instruments, and anonymous products.
    - **Customer Risk**: Low financial inclusion, person-to-person remittances, and online impersonation risks.
2. **Core Principles**:
    - **Know Your Customer (KYC)**: Central to AML compliance, involving due diligence and ongoing monitoring.
    - **Risk-Based Approach (RBA)**: Financial institutions assess risks and implement proportionate controls.
    - **Customer Due Diligence (CDD)**: Five levels of diligence, from anonymous to enhanced monitoring and suspicious activity reporting (SAR).
3. **Automated Monitoring**:
    - Jube supports real-time and batch processing for transaction monitoring.
    - Focus on anomaly detection and classification using supervised and unsupervised machine learning techniques.
    - Activation rules escalate suspicious cases for further investigation.
4. **Data-Driven Risk-Based Approach**:
    - Jube uses risk factors such as product characteristics, transaction behaviour, and geographic spending patterns.
    - Machine learning models (e.g., One-Class SVM) identify anomalies and classify suspicious activities.
    - Risk factors are modelled using abstraction rules and integrated into activation rules for case escalation.
5. **Case Management**:
    - Cases flagged by rules are reviewed by analysts, with statuses like "Refer to MLRO," "No Further Action," or "SAR Sent."

- Robust audit trails ensure transparency, and EDD documentation can be uploaded for further investigation.
- Escalation to the Money Laundering Reporting Officer (MLRO) and SAR creation are streamlined.

6. **MLRO Dashboards**:
   - Provide real-time insights into product behaviour, customer activity, and territorial risks.
   - Enable initiative-taking risk management and adaptation to emerging threats.
7. **Integration and Data Processing**:
   - Jube integrates data from various sources (e.g., MasterCard/Visa authorizations, financial transactions, and CDD events).
   - IP address decoding provides geographic and contextual insights for risk assessment.
   - Data is processed serially, even in batch mode, to simulate real-time monitoring.
8. **Value Proposition**:
   - **Cost Reduction**: Eliminates prohibitive costs of proprietary solutions.
   - **Vendor Lock-In Eradication**: Open-source nature ensures flexibility.
   - **Improved Compliance**: Advanced tooling enhances regulatory adherence.

Key Features of Jube:

- **Real-Time Processing**: Ensures timely detection of suspicious activities.
- **Open-Source Advantage**: Transparency, customization, and cost efficiency.
- **Adaptability**: Supports evolving AML regulations and emerging risks.
- **Advanced Analytics**: Combines supervised and unsupervised learning for robust risk detection.

Jube provides a powerful, flexible, and cost-effective solution for AML transaction monitoring. By leveraging its real-time capabilities, advanced analytics, and open-source nature, financial institutions can enhance compliance, reduce costs, and adapt to evolving financial crime threats. The framework emphasizes a data-driven, risk-based approach, ensuring effective monitoring and regulatory alignment.