|  |
| --- |
| DataScience MiddleEast  3-6-2025 |

|  |
| --- |
|  |
| Business Requirements Document – SAS Fraud Detection |
| Khaleeji Bank (Bahrain) / Phase One  A black and grey logo  AI-generated content may be incorrect. |

Contents

[Document Purpose 3](#_Toc192414150)

[About the Project 3](#_Toc192414151)

[1 Message Classifications 5](#_Toc192414152)

[2 Alert Types 7](#_Toc192414153)

[3 Organisations 8](#_Toc192414154)

[4 Projects 9](#_Toc192414155)

[5 Advanced Lists 10](#_Toc192414156)

[6 Domains 11](#_Toc192414157)

[7 Triage Types 12](#_Toc192414158)

[8 Queues 13](#_Toc192414159)

[9 Dispositions 17](#_Toc192414160)

[9.1 Mapping Dispositions to Queues 19](#_Toc192414161)

[10 Rules 20](#_Toc192414162)

[11 Reports Requirement 20](#_Toc192414163)

[11.1 Out Of The Box Reports 20](#_Toc192414164)

[11.1.1 Fraud Detection 20](#_Toc192414165)

[11.1.2 Fraud Summary 20](#_Toc192414166)

[11.1.3 Active Alerts 21](#_Toc192414167)

[11.1.4 Frequency of Rules 22](#_Toc192414168)

[11.1.5 Performance Summary 23](#_Toc192414169)

[11.2 Custom Reports 24](#_Toc192414170)

[11.2.1 Financial Alerts 24](#_Toc192414171)

[11.2.2 Non-Financial Alerts 26](#_Toc192414172)

[11.2.3 Rules Efficiency 28](#_Toc192414173)

[11.2.4 Transaction Threshold 29](#_Toc192414174)

# Document Purpose

This document is intended to capture the customer’s preferences in configuring SAS Detection Architecture prior to its installation, so that it may be used as a guide for its intended audience. This includes the customer’s IT group and their business operations group, as both will need to work together to ensure that the system configuration is aligned with the business needs. This document contains specific items to be agreed by the business that relate directly to how these users shall interact with the system.

# About the Project

This section can be completed by the customer. This is to provide a summary of who is involved in the project.

Organization:

List down the key individuals for the business planning sessions. These individuals have the authority to plan, discuss, and make changes to the project.

Table 1: Project Organization Structure

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Business Title** | **Contact details (phone and eMail)** | **Role in project** |
| **Project team** | | | |
| Mohamed Abdelghany | SFD SME | Mohamed.abdelghany@datascience.me |  |
| Tahseen Shaier | Project Manager | Tahseen.Shaier@datascience.me |  |
| Mahmoud Yassin | Senior SFD Consultant | Mahmoud.Yassin@datascience.me |  |
| Amal Ibrahim | Service Delivery Manager | [Amal.Ibrahim@datascience.me](mailto:Amal.Ibrahim@datascience.me) |  |
| Mostafa Hasanin | Software Engineer | [Mostafa.hasanin@datasicence.me](mailto:Mostafa.hasanin@datasicence.me) |  |
| Mennatallah El-Sharkawy | Data Analyst | menna.sharkawy@datascience.me |  |
| Asmaa Abouelfotouh | Data Analyst | asmaa.abouelfotouh@datascience.me |  |
| **Business team** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **IT team** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Operations team** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Revision History

| Version | By | Date | Description |
| --- | --- | --- | --- |
| 1.0 | Mahmoud Yassin | 06/03/2025 | - Initial Draft |
| 1.1 | Mohamed Youssef Amal Saleh  Asmaa Abouelfotouh | 09/03/2025 | * Add reports * Adjust document layout |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Glossary

Describes acronyms and abbreviations used in this document.

|  |  |
| --- | --- |
| **Acronym/Abbreviation** | **Description** |
| IT | Information Technology |
| KB | Khaleeji Bank |
| SFD | SAS Fraud Decisioning |
| Third Party | Entity that is involved in some way in an interaction between two other entities |
| BRD | Business Requirements Document |
| Info | Information |

# 1 Message Classifications

Message classification hierarchies are a way of arranging message allocation nodes, organizations, projects, and rules. Message classification hierarchies help you to visualize which organizations, projects, and rules process specific messages. You are allowed one message classification hierarchy per SAS Viya 4 tenant.

A message classification hierarchy is populated with message classification nodes. The message classification nodes that make up a message classification hierarchy are arranged into levels. A message classification hierarchy can have up to 8 levels. The first level in a message classification hierarchy is always a single Global message classification node. You can then associate in the second level up to 9999 message classification nodes stemming from this Global message classification node. Each of the message classification nodes that appear in that second level can then associate up to 9999 message classification nodes with them in the third level. This pattern can then be repeated in the remaining 5 levels.

See SAS Detection Architecture Administor’s Guide -> Message Classifications for more information.

Click on the following diagram to build your own Message Classification. Remember that there can be a maximum of 8 levels (vertical) and 9999 child nodes per level (horizontal).

Figure 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Code** | **Name**  **The internal short name of the message classification. Contains string values of up to 16 characters. Valid values include letters, numbers, hyphens, and underscores.** | **Display Name**  **The descriptive name of the message classification. Contains string values of up to 75 characters.** | **Created By**  **(Optional) The user ID that created the message classification. Contains string values of up to 40 characters.** |
| 1 | GLOBAL | GLOBAL | Admin user |
| 1.1 | Khaleeji | Khaleeji | Admin user |
| 1.1.1 | Customer | Customer | Admin user |

# 2 Alert Types

Administrators can define as many Alert Types as required. Each Alert Type is unique and is used in identifying crucial information about the alert. Alert Types facilitate this by specifying the variable paths on the incoming message to the Triage System (SAS Alert Triage) which it will use to source information about the alert. For instance, Alert Types specify the type of entity that the alert will be generated on as well as the Parent and Contact entities for that alert.

Entities are not classified as being Parent and Contact entities as part of the entity definitions but are instead specified on a per-Alert Type level. A Parent entity is considered to be the entity that is directly related to the entity being alerted on, while the contact entity is the entity that users within the system would use to identify the information required to establish contact with the owner of the alerted entity.

The same entity can therefore play the role of the alerted entity, the Parent entity as well as the Contact entity across multiple alert types. While all Alert Types must have an alerted entity, or actionable entity, type specified they do not require either a Parent or Contact entity type to be specified.

Note: An actionableEntityVariablePath is not required as SAS Alert Triage will always pull the ID of the alerted entity from the alert’s outcome entity variable which is on the alert recommendation message.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Alert Type ID** | **Alert Type Name** | **Code** | **Actionable Entity Type Id** | **Contact Entity Type ID** | **Contact Entity Variable** | **Parent Entity Type ID** | **Parent Entity Variable** | **Domain ID** |
| **Unique identifier for an Alert Type.** | **The display value for this alert type that will be used within user interface.**  **Max 100 characters** | **The value on incoming alerts that will be used to tie the alert recommendation to an Alert Type. Max 15 characters .Must be unique** | **The entity type that alerts of this type will be alerting on.** | **Optional - the ID of an existing Entity Type that will serve as the Contact Entity** | **Optional – the message schema variable where the ID of the contact entity is found on the alerted transaction.** | **Optional - the ID of an existing Entity Type that will serve as the Parent Entity** | **Optional – the message schema variable where the ID of the parent entity is found on the alerted transaction.** | **The domain that the alert type is associated with** |
| KB\_customer | Customer | KB\_customer | KB\_customer | KB\_customer | message.customer.identifier | KB\_customer | message.customer.identifier | online\_fraud |

# 3 Organisations

The highest layer of an implementation is a SAS Viya 4 tenant. A tenant is a user or an organization with shared access to a software instance. Everything that exists within one tenant is wholly separate from anything that exists or occurs within another tenant. This means that everything, from the clusters to the individual rules in tenant A cannot be referenced or used by tenant B.

Organizations are the highest level of grouping within a SAS Viya 4 tenant. The stated purpose of an organization is to solve specific business decisioning problems. Each tenant can have as many organizations as needed, provided that there is enough resourcing available to have them all run.

Organizations do not share any information across their boundaries, despite sharing resources.

Every organization within a SAS Viya 4 tenant has access to the same list of alert types and message schemas.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Organisation Display Name**  The name can be up to 75 characters in length | **Organisation Name**  Valid characters include letters, numbers, hyphens, underscores, and spaces. The name can be up to 16 characters in length. | **Description**  This field accepts up to 1000 characters. | **Message Classification Node**  The message classification to which the organization is to be assigned | **Message Schema**   An organization must include at least one message schema. |
|  |  |  |  |  |
| KhaleejiOrg | KhaleejiOrg | KhaleejiOrg | GLOBAL | Card Fraud  Payment Fraud |

# 4 Projects

Projects are the distilled lines of business that you work on. Each base organization can have many projects, but each project can be associated with only a single base organization. All of the content that is available to a project is determined by what is associated with that base organization.

A project can contain all or only a subset of the message schemas, users, and profile variables that are associated with the organization.

Projects within an organization cannot have the same name. Projects in different organizations can have the same name.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Organisation Name** | **Project Name**  Valid characters include letters, numbers, hyphens, underscores, and spaces. You can enter up to 256 characters | **Description**  This field accepts up to 1000 characters. | **Users** | **Message Classification Node**  The message classification that the project is assigned | **Message Schema**   A project must include at least one message schema. |
| KhaleejiOrg | Khaleeji Fraud Project |  | Admin user | Global | Card Fraud  Payment Fraud |

# 5 Advanced Lists

|  |  |  |  |
| --- | --- | --- | --- |
| **Organisation Name** | **Advanced List Name** | Advanced List Label  Optional | Advanced List Description  Optional |
| KhaleejiOrg | Public Holidy | Public Holidy | Public Holiday List |
| KhaleejiOrg | Restricted Nationalities | Restricted Nationalities | Restricted Nationalities List |
| KhaleejiOrg | Blacklisted IBANs | Blacklisted IBANs | Blacklisted IBANs List |
| KhaleejiOrg | Blacklisted Mobile Numbers | Blacklisted Mobile Numbers | Blacklisted Mobile Numbers List |

# 6 Domains

Domains are the highest organizational concept within SAS Alert Triage. A system can have as many Domains defined as required. It allows the grouping and isolation of Triage types and Alert types.

Domains act as a boundary between Alert Types, meaning that each Alert Type specified in SAS Alert Triage is directly tied a single Domain.

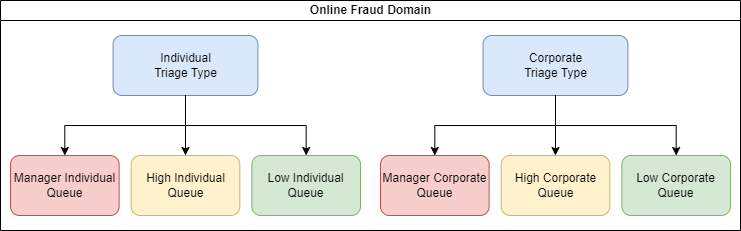


Figure 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain ID**  **(Unique identifier for a Domain)** | **Domain Name**  **(Display label that will be surfaced within the user interface)** | **Description**  **(Description for a given Domain. Max 500 characters)** | **Default Flag**  **(Specifying whether the information will be used to update the details of the Default Domain)** |
| Online\_Fraud\_Domain | Online Fraud Domain |  | true |

# 7 Triage Types

Triage Types represent the second level within the SAS Alert Triage structural hierarchy. A Triage Type can only be associated with a single Domain but can have multiple Queues associated to it.

Triage types are associated back to Domains and act as means to group Queues. The following concepts are directly associated with Triage Types​

* Page layouts​
* Triage grid (search layout) definitions ​
* Triage type servicing priorities ​
* Queues

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Triage Type**  **(unique identifier for a Triage Type)** | **Triage Type Name**  **(display label that will be surfaced within the user interface Max 100 characters)** | **Domain ID**  **(the ID of an existing Domain definition with which this Triage Type will be associated.** | **Triage Type Description**  **(description for a given Triage Type)** | **Triage Mode**  **(currently needs to be set to “MANUAL” on all Triage Types.)** | **Service Priority**  **(Each Triage Type must have a unique servicing priority per Domain . Minimum value: 1. Maximum value: 32767)** | **Default Flag**  **(specify whether the information specified will be used to update the details of the Default Triage Type)** |
| Individual Triage Type | Individual Triage Type | Online\_Fraud\_Domain |  | MANUAL | 1 | true |
| Corporate Triage Type | Corporate Triage Type | Online\_Fraud\_Domain |  | MANUAL | 2 | false |

# 8 Queues

Queues within SAS Alert Triage are used to store incoming Alerts. Queues are arranged under Triage Types. Each Triage Type can have one or more Queues associated with it while a Queue can only be associated with a single Triage Type.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Description** | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 |
| **Queue ID** | **Unique identifier for a Queue** | High Individual Queue | Low Individual Queue | Manager Individual Queue | High Corporate Queue | Low Corporate Queue | Manager Corporate Queue |
| **Queue Name** | **Display value for a Queue that will be used within user interface** | High Individual Queue | Low Individual Queue | Manager Individual Queue | High Corporate Queue | Low Corporate Queue | Manager Corporate Queue |
| **Default Flag** | **Specifying whether the information will be used to update the details of the Default Queue.** | false | true | false | false | false | false |
| **Domain ID** | **ID of an existing Domain associated with the Triage Type that the Queue is in** | Online\_Fraud\_Domain | Online\_Fraud\_Domain | Online\_Fraud\_Domain | Online\_Fraud\_Domain | Online\_Fraud\_Domain | Online\_Fraud\_Domain |
| **Triage Type ID** | **ID of an existing Triage Type definition that the Queue will be associated with** | Individual Triage Type | Individual Triage Type | Individual Triage Type | Corporate Triage Type | Corporate Triage Type | Corporate Triage Type |
| **Service Priority** | **Assigning a servicing priority to a Queue. Each Queue must have a unique servicing priority per Triage Type. Minimum value: 1. Maximum value: 32767** | 2 | 3 | 1 | 2 | 3 | 1 |
| **Routing Priority** | **Assigning a Routing Priority to a Queue. Each Queue must have a unique Routing Priority per Triage Type. Minimum value: 1, Maximum value: 32767** | 2 | 3 | 1 | 2 | 3 | 1 |
| **Service Sort Field Order** | **Alerting field that will be used to sort alerts in the Queue for the purposes of Servicing. The sort order is parameterized as either “ascending” or “descending”.**   * **Max 500 characters** * **Defaults to creationTimeStamp:ascending** | creationTimeStamp:ascending | creationTimeStamp:ascending | creationTimeStamp:ascending | creationTimeStamp:ascending | creationTimeStamp:ascending | creationTimeStamp:ascending |
| **Service Enabled** | **Defines whether the alerts in the Queue will be considered when the system determines the next alert to surface to a user. Defaults to false** | true | true | true | true | true | true |
| **Routing Enabled** | **Define whether incoming alerts can be routed to into a Queue or not. This property supports a value of either “true” or “false. Defaults to “true”. Alerts being moved into a Queue because of a Disposition will not be prevented from being moved into a Queue that has this property set to “false”.** | true | true | true | true | true | true |
| **Alert Max Duration in Queue** | **The maximum amount of time that an alert will remain in a Queue before having its status changed to “CLOSED” by the system. The *alertMaxDurectionInQueue* property accepts an integer value that specifies the amount of time, in hours. Defaults to 24** | 8760 | 8760 | 8760 | 8760 | 8760 | 8760 |
| **Sticky Flag** | **Define whether alerts can be moved out of a Queue by the system. A Queue that has a value of “true” will prevent alerts from being routed into another Queue by the system. User initiated moves are not prevented by this property being set to “true”. Defaults to “false”** | false | false | false | false | false | false |

# 9 Dispositions

A Disposition within SAS Alert Triage is a point-in-time decision about how a given alert should be handled. A Disposition references a collection of one or more Action Grouping definitions which, in turn, is comprised of one or more Actions. When a Disposition is applied to an alert all of the Actions associated with the Action Groupings referenced by the Disposition are carried out by the system.

Dispositions are associated to Queues. A Disposition can be associated with multiple Queues and a Queue can be associated to multiple Dispositions. A Disposition is available to be enacted on any alert that is stored within the alert with which that Disposition is associated. A Disposition can only be enacted on an Alert by a user if that user has the lock on the alert, with the exception of an Alert being dispositioned via Bulk Dispositioning.

A screenshot of a computer

Description automatically generated

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Disposition ID** | **Disposition Name** | **Description** | **Action Group ID** | **Bulk Apply Flag** |
| **Unique Identifier for the Disposition** | **Display label for a Disposition that will be surfaced to users** | **Description that appears within the “Dispositioning” panel that is displayed to a user** | **ID of the Action Group definition associated with the Disposition** | **Whether a Disposition is available to be used as part of a bulk dispositioning action. The property supports values of “true” and “false”. Dispositions with a property value of “true” are still available to be applied by users applying a Disposition via the “Dispositioning” panel.** |
| Close immediately | Close immediately | Close immediately | close-alert | false |
| Close an alert after 1 hour | Close an alert after 1 hour | Close an alert after 1 hour | auto-close-alert | false |
| Close alert at specified date and time | Close alert at specified date and time | Close alert at specified date and time | interactive-auto-close-alert | false |
| Close as Productive | Close as Productive | Close as Productive | auto-close-alert  set-productivity-rating | false |
| Close as Unproductive | Close as Unproductive | Close as Unproductive | auto-close-alert  set-productivity-rating | false |
| Close as Indeterminate | Close as Indeterminate | Close as Indeterminate | auto-close-alert  set-productivity-rating | false |
| Reactivate Immediately | Reactivate Immediately | Reactivate Immediately | reactivate-alert | false |
| Suspend an alert for 1 hour | Suspend an alert for 1 hour | Suspend an alert for 1 hour | suspend-alert | false |
| Suspend alert until specified date and time | Suspend alert until specified date and time | Suspend alert until specified date and time | interactive-suspend-alert | false |
| Reroute to another Queue | Reroute to another Queue | Reroute to another Queue | interactive-move-to-queue | false |

### 9.1 Mapping Dispositions to Queues

|  |  |
| --- | --- |
| **Queue ID** | **Disposition ID** |
| High Individual Queue  Low Individual Queue  Manager Individual Queue  High Corporate Queue  Low Corporate Queue  Manager Corporate Queue | Close immediately  Close an alert after 1 hour  Close alert at specified date and time  Close as Productive  Close as Unproductive  Close as Indeterminate  Reactivate Immediately  Suspend an alert for 1 hour  Suspend alert until specified date and time  Reroute to another Queue |

# 10 Rules

In the attached sheet below are the list of discussed and agreed rules to be applied in the SFD solution



Sheet 1 The confirmed list of Rules with their specs

# 11 Reports Requirement

## Out Of The Box Reports

### 11.1.1 Fraud Detection

The metrics provided in the fraud detection report provide a summary of potential fraud exposure daily.

| **Business Field Name** | **Report Filter**  **Multiple / single selection** | **Calculation Logic** |
| --- | --- | --- |
| Alert Type | YES | Direct map |
| Fraud Entity | YES | Direct map |
| Domain | YES | Direct map |
| Triage Type | No | Direct map |
| Queue | YES | Direct map |

### Fraud Summary

The fraud summary report determines the effectiveness of each queue by measuring the number of detected frauds in each queue by fraud type on a daily basis.

|  |  |  |
| --- | --- | --- |
| **Business Field Name** | **Report Filter** | **Calculation Logic** |
| Alert Type | YES | Direct map |
| Queue | YES | Direct map |
| non-productive(Negative response) | NO | Calculated based on the disposition status |
| productive(Positive response) | NO | Calculated based on the disposition status |
| Number of Closed Alerts | NO | Calculated based on the alert status |
| Triage Type | NO | Direct map |

### Active Alerts

Active Alerts report provides a report of how many alerts are pending action in the system and their Age since creation on a daily basis.

|  |  |  |
| --- | --- | --- |
| **Business Field Name** | **Report Filter**  **Multiple / single selection** | **Calculation Logic** |
| Alert Status | NO | Direct map |
| Active Alerts Count | NO | Direct map |
| Triage Type | NO | Direct map |
| Alert Type | YES | Direct map |
| Queue | YES | Direct map |
| Alert Age | NO | Calculated item based on the alert created date |

### Frequency of Rules

The frequency of the rules firing report provides a report of how many alerts were created by each rule that was included in the report on a daily basis.

|  |  |  |
| --- | --- | --- |
| **Business Field Name** | **Report Filter**  **Multiple / single selection** | **Calculation Logic** |
| Rule ID | YES | Direct map |
| Rule Description | YES | Direct map |
| Rule Name | YES | Direct map |
| Rules Fired Count | YES | Direct map |
| Triage Type | YES | Direct map |
| Queue | YES | Direct map |
| Alert Type | YES | Direct map |
| Message Classification Name | NO | Direct map |

### Performance Summary

The system performance summary report provides a breakdown of the types of fraudulent activity for the alerts that were given a confirmed risk status on a daily basis.

|  |  |  |
| --- | --- | --- |
| **Business Field Name** | **Report Filter**  **Multiple / single selection** | **Calculation Logic** |
| Rule ID | NO | Direct map |
| Rule Name | YES | Direct map |
| Triage Type | YES | Direct map |
| Queue | YES | Direct map |
| Alert Type | YES | Direct map |
| Message Classification Name | YES | Direct map |
| non-productive(Non-fraud Count) | YES | Direct map |
| productive(Other Fraud Count) | YES | Direct map |
| Rule ID | YES | Direct map |



Sheet 2 The templates of the OOTB Reports

## Custom Reports

### 11.2.1 Financial Alerts

Provide insights about the Financial Rules alerts daily.

|  |  |  |
| --- | --- | --- |
| **Business Field Name** | **Report Filter**  **Multiple / single selection** | **Calculation Logic** |
| Alert ID |  | Direct map |
| Alert Status | YES | Direct map |
| Alert Create Date | YES | Direct map |
| Last Assigned User |  | Direct map |
| Alert age calculated |  | Calculated based on alert created date |
| Rule ID |  | Direct map |
| Rule Name | Multiple Selection | Direct map |
| Domain Name | Yes | Direct map |
| Alert Type |  | Direct map |
| Triage Type | Yes | Direct map |
| Entity ID | Yes | Direct map |
| Entity Type | Yes | Direct map |
| Entity Name |  | Direct map |
| Age |  | Calculated based on customer birth date |
| Mobile Number |  | Direct map |
| Account Number |  | Direct map |
| Account Type | Yes | Direct map |
| Transaction Datetime |  |  |
| Transaction amount |  |  |
| Transaction Channel |  |  |
| Passport Number |  | Direct map |
| Employer Name |  | AML |
| Assessment Type | Yes | Direct map |
| Alert Close Date |  | Direct map |
| last updated on |  | Calculated based on the refresh time of the data |
| Nationality | Yes | Direct map |

### Non-Financial Alerts

Provide insights about the Non-Financial Rules alerts on a daily basis.

|  |  |  |
| --- | --- | --- |
| **Business Field Name** | **Report Filter**  **Multiple / single selection** | **Calculation Logic** |
| Alert ID |  | Direct map |
| Alert Status | YES | Direct map |
| Alert Create Date | YES | Direct map |
| Alert age calculated |  | Direct map |
| Rule ID |  | Direct map |
| Rule Name | Multiple Selection | Direct map |
| Domain Name | YES | Direct map |
| Alert Type |  | Direct map |
| Triage Type | YES | Direct map |
| Entity ID | YES | Direct map |
| Entity Type | YES | Direct map |
| Entity Name |  | Direct map |
| Age |  | Direct map |
| Mobile Number |  | Direct map |
| Device Information |  |  |
| IP Address |  |  |
| IP Location |  |  |
| Access Datetime |  |  |
| Transaction Channel |  |  |
| Account Type | YES | Direct map |
| Passport Number |  | Direct map |
| Employer Name |  | AML |
| Assessment Type | YES |  |
| Alert Close Date |  | Direct map |
| last updated on |  | Direct map |
| Nationality | Yes | Direct map |

### Rules Efficiency

Provide insights about all the rules in the system and measure the performance of the rules on a daily basis.

|  |  |  |
| --- | --- | --- |
| **Business Field Name** | **Report Filter**  **Multiple / single selection** | **Calculation Logic** |
| Rule ID |  | Direct map |
| Rule Name | Multiple Selection | Direct map |
| Rule Description |  | Direct map |
| Transaction Type |  | Direct map |
| Alert Entity Type |  | Direct map |
| Action Required |  |  |
| Threshold |  | Direct map |
| Number of Alerts Triggered |  | Direct map |
| Number of CIF affected |  | Direct map |
| Transaction amount (aggregated) |  | Direct map |
| Confirmed / False Positive ( Alerts ) |  | Direct map |

### Transaction Threshold

Provide insights about specific types of transactions on a weekly basis.

|  |  |  |
| --- | --- | --- |
| **Business Field Name** | **Report Filter**  **Multiple / single selection** | **Calculation Logic** |
| CIF ID | YES | Direct map |
| CIF Type | Yes | Direct map |
| Account Name |  | Direct map |
| Nationality | YEs | Direct map |
| Age |  | Direct map |
| Mobile Number |  |  |
| Account Number | yes | Direct map |
| Total debits ( based on the date selection) |  |  |
| Total credits ( based on the date selection) |  |  |
| Transaction Channel |  |  |
| Passport Number |  | Direct map |
| Account Type | Yes | Direct map |
| Employer Name |  | AML |
| Rule ID |  | Direct map |
| Rule Name | YES | Direct map |
| Alert ID |  | Direct map |
| Alert Status | YES | Direct map |
| Alert Create Date | YES | Direct map |
| Account Type | Yes | Direct map |

****

Sheet 3 The template of customized reports