Oracle® FCCM Know Your Customer Cloud Service

Technical Scenario Descriptions

Release 24.2.1
F96213-01
February 2024

Oracle FCCM Know Your Customer Cloud Service Technical Scenario Descriptions, Release 24.2.1

F96213-01

Contents

Preface

Audience iv
Help iv
Documentation Accessibility iv
Diversity and Inclusion iv
Related Resources v
Conventions v
Comments and Suggestions v

1 Introduction

2 How to Read the Technical Scenario Descriptions

2.1 Technical Scenario Description Components 2-1

3 Risk Factor Scenarios in KYC

3.1 KYC Transaction Based Risk Factors 3-1

Preface

Technical Scenario Descriptions describes the Know Your Customer Cloud Service Technical Scenario Descriptions.

Audience

This document is intended for users who are responsible for provisioning and activating Oracle FCCM Know Your Customer Cloud Service or for adding other users who would manage the services, or for users who want to develop Oracle Cloud applications.

Help

Use Help Icon  to access help in the application. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. Not all pages have help icons. You can also access the https://docs.oracle.com/en/ to find guides and videos.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

For more information, see these Oracle resources:

- Oracle Public Cloud: http://cloud.oracle.com
- Community: Use https://community.oracle.com/customerconnect/ to get information from experts at Oracle, the partner community, and other users.
- Training: Take courses on Oracle Cloud from https://education.oracle.com/oracle-cloud-learning-subscriptions.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: https://support.oracle.com/portal/.

1 Introduction

Oracle Financial Services Crime and Compliance Management Know Your Customer Cloud Service (FCCM KYC Cloud Service) performs risk assessment for a customer & related parties using a variety of risk factors including demographic, product, geography, watch list matches etc. To further enhance the risk scoring model, the system will now support behavioral based risk factors which are derived based on transactional activity across products and channels. These behavioral risk factors can be used as part of Business Check and Algorithm-based risk scoring models for deployment initiation & daily batch processing.

2

How to Read the Technical Scenario Descriptions

This section describes the layout (a description of the headings) of each technical scenario description, and explains how to read the information and its style notes. Each technical scenario description has the structure defined in the following sections.

2.1 Technical Scenario Description Components

For client-created scenarios, filters, risk indicators, and thresholds can be adjusted at any time using the Pipeline Designer. To adjust out of the box scenarios, you must first copy the scenario, then configure the copied scenario.

The technical scenario description components are as follows:

- **Scenario Name**
- **Data of Interest**
- **Filters**
- **Risk Indicators**
- **Thresholds**

Scenario Name

This section provides the scenario name as it displays in the user interface (UI). This is typically the scenario's abbreviated name. This section defines the behavior that the scenario is designed to detect, and explains how this behavior pertains to a specific entity type.

Data of Interest

This section lists the types of information used by the scenario for event generation or display. Essentially, this is the data that the system uses to detect unusual or suspicious behavior.

Filters

This section lists any applicable inclusions and exclusions for the scenario, such as the focus and the exclusionary parameters. Filters represent pre-set values defined for various data points within the Data of Interest. Filters cross threshold sets and are applied equally to filter the data of interest.

Risk Indicators

Risk Indicator widget is used to configure various behavioral based risk factors for different entity types (In case of KYC it is primarily customer focused). Users can configure various risk factors using a variety of transaction types say cash transactions, wire transfers, online payments, card payments etc. This widget allows users to configure risk factors using a variety of normal operators, aggregate functions, and custom expressions.

Thresholds

This section contains tables with the tunable thresholds that are built into the scenario. Applicability of Thresholds is specified in the Focus column in the threshold table.

The following terms are used as column headers in these tables:

- **Threshold Name**: This shows the threshold name that displays in the Threshold Editor in the UI.
- **Description**: This provides an explanation of the threshold.
- **Focus**: When applicable, this column defines the focus to which the threshold applies.
- **Frequency Period**: This is the default frequency of the detection process and it is indicated in days. Typically, the frequency period is tunable. If the frequency period should be restricted, minimum and maximum values are provided.
  In general, the frequency period is used to avoid generating duplicate alerts for the same focal entity from the same scenario. Between the detection process runs on a scenario, new business data records are ingested, and then covered by the next detection process run to generate a new alert. To avoid duplicate alerts across scenario runs, a new alert must have at least one transaction which has occurred within the Frequency Period and which has contributed to the alert being generated. You can set how frequently a scenario is run through the Scheduler Service. For more information about how to schedule and run scenarios, see Using Scheduler Service.
- **Lookback Period**: This is the default timespan of data monitored in each run of the detection process. In general, the Lookback Period is tunable. In cases when the Lookback Period must be restricted, the minimum and maximum values are provided. It is possible that the Frequency Period may be less than the Lookback Period.
  For example, if the Lookback Period was seven days, the scenario would lookback at the last seven days' worth of data (including the current day), and run its detection process on that data.

3
Risk Factor Scenarios in KYC

This section describes the KYC Transaction Based Risk Factor scenarios.

3.1 KYC Transaction Based Risk Factors

Use the **KYC Risk Factor** pipeline type for creating these scenarios.

The following is an out-of-the-box scenario pipeline.

- **Scenario Name**
- **Data of Interest**
- **Filters**
- **Risk Indicators**
- **Events**
- **Thresholds**

Scenario Name

KYC Transaction Based Risk Factors

Data of Interest

Data of Interest represents the types of business information required for this scenario to be effective.

For KYC, the following are used:

- Front Office Transaction
- Front Office Transaction Party
- Back Office Transaction

Filters

Filters represent pre-set values defined for various data points within the Data of Interest. Filters cross threshold sets and are applied equally to filter the data of interest.

Table 3-1 Filters for KYC Transaction Based Risk Factors

Parameter Name	Description	Sample Value
KYC Risk Factor Focused	Indicates that this scenario pipeline is for KYC.	Yes/No **Note**: The value must be Yes for this Pipeline type.
Transaction Type	Indicates which types of transactions should be included when risk scoring a customer.	Wire, Cash.

Risk Indicators

Risk Indicators define factors that can be used in the scenario logic to determine whether a behavior matches the definition of risky behavior as defined by the scenario objective.

Table 3-2 Risk Indicators for KYC Transaction Based Risk Factors

Risk Indicator	Description
Credit Txn Amount in last Twelve months	Indicates the total amount of the credit transactions during the last twelve months.
Debit Txn Amount in last Twelve months	Indicates the total amount of the debit transactions during the last twelve months.
Total Cash Txn Amount in last Twelve months	Indicates the total amount of cash transactions during the last twelve months.
Total Cash Txn Count in last Twelve months	Indicates the total number of cash transactions during the last twelve months.
Total Cash Txn Count in last Twelve months	Indicates the total number of cash transactions during the last twelve months.
Credit Txn Count in last Twelve months	Indicates the total number of credit transactions during the last twelve months.
Debit Txn Count in last Twelve months	Indicates the total number of debit transactions during the last twelve months.
Total Txn Amount in last Twelve months	Indicates the total transaction amount during the last twelve months.
Total Txn Count in last Twelve months	Indicates the total number of transactions during the last twelve months.
Total Cash Txn Vs Total Txn Count in last Twelve months	Indicates the ratio of total cash transactions to the total number of transactions during the last twelve months.
Total Cash Txn Vs Total Txn Amt in last Twelve months	Indicates the ratio of total cash transactions to the total transaction amount during the last twelve months.
Incoming HRJ Wire Txn Count in last Twelve months	Indicates the total number of incoming wire transactions from a high risk jurisdiction during the last 12 months

Events

For KYC Risk Factor scenarios, Events is used to persist the final computed values of each risk indicators in a temporary output table consumed by KYC. These values are further used by the KYC to compute the final risk scores of the customers.

Thresholds

This section contains tables with the tunable thresholds that are built into the scenario.

Table 3-3 Thresholds for KYC Transaction Based Risk Factors

Threshold	Description	Sample Value
Jurisdiction	The list of jurisdiction codes that the scenario covers. The client defines allowable values.	AMEA
Look back Period	Number of months prior to the current month specified for the look back period.	12
Frequency Period	Set this value to 1. **Note**: For KYC, the risk factors are computed as and when the customer is picked up for risk assessment.	1