Know Your Customer
Administration Guide

Release 2.0
June 2013

ORACLE®

FINANCIAL SERVICES

ORACLE®

Know Your Customer
Administration Guide

Release 2.0
June 2013

Document Control Number: 9MN12-2.0-0007
Document Number: AG-13-KYC-0001-2.0-02

Contents

Contents

List of Figures

List of Figures

List of Tables

About This Guide

This guide provides comprehensive instructions for proper system administration, and the daily operations and maintenance of the OFS KYC. The logical architecture provides details of the KYC process for a better understanding of the pre-configured application, which allows you to make site-specific enhancements using OFSAAI. This chapter contains the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information
- Conventions Used in this Guide

Who Should Use this Guide

The *Oracle Financial Services KYC Administration Guide i*s designed for Oracle Financial Services Installers and System Administrators. Their roles and responsibilities, as they operate within the Oracle Financial Services KYC, include the following:

- **Oracle Financial Services KYC Installer:** Installs and configures the Oracle Financial Services KYC at a specific deployment site. The Oracle Financial Services KYC Installer also handles customer specific enhancements or changes and accesses information about deployment-specific configuration (for example, machine names, port numbers, and business metadata).

- **System Administrator:** Configures, maintains, and adjusts the system and is usually an employee of a specific Oracle Financial Services customer. The System Administrator maintains user accounts and roles, monitors data ingestion and case management, archives data, loads data feeds, and performs post-processing tasks.

How this Guide is Organized

The *Oracle Financial Services KYC Administration Guide* includes the following chapters:

- Chapter 1, *KYC Architecture Overview* provides a brief overview of the Oracle Financial Services KYC architecture and operations.
- Chapter 2, *KYC Operations,* details the Application Operations of the KYC.
- Chapter 3, *Views,* details the Oracle database view definitions to process risk assessment requests.
- Chapter 4, *Functions, Stored Procedures and Packages,* details the functions and stored procedure definitions to process risk assessment requests.
- Appendix A, *KYC Batches,,* covers the KYC Batch and the tasks within the batches.
- Appendix B, *Excel Upload Templates,,* describes the templates used by the Excel Upload feature.
- Appendix C, *Configurability,,* describes how to configure the Oracle Financial Services KYC.
- Appendix D, *Extraction Definition,,* describes the delimiters used to extract.

- Appendix E, *Resaving Runs,*, describes how to save and resave runs.

- Appendix F, *KYC Batch Execution Logs,*, provides the information of where log files are created for each type of task in the Oracle Financial Services KYC.

Where to Find More Information

For more information about Oracle Financial Services KYC, refer to the following documents:

- *Enterprise Case Management User Guide*:

- *KYC Risk Assessment Guide*

- *Configuration Guide*

- *Installation Guide - Stage 1*

- *Installation Guide - Stage 3*

- *Services Guide*

To find additional information about how Oracle Financial Services solves real business problems, see our website at www.oracle.com/financialservices.

Conventions Used in this Guide

Table 1 lists the conventions used in this guide.

Table 1. Conventions Used in this Guide

Convention	Meaning
Italics	●Names of books, chapters, and sections as references ●Emphasis
Bold	●Object of an action (menu names, field names, options, button names) in a step-by-step procedure ●Commands typed at a prompt ●User input
`Monospace`	●Directories and subdirectories ●File names and extensions ●Process names ●Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
<Variable>	Substitute input value

CHAPTER 1　*KYC Architecture Overview*

This section provides a brief overview of the Oracle Financial Services KYC architecture and operations. This chapter focuses on the following topics

- About Oracle KYC Architecture
- OFSAAI Architecture
- Deployment View

About Oracle KYC Architecture

Oracle Financial Services Know Your Customer is built on the OFSAAI Platform. You can think of architecture as a blueprint of parts that fit together to define a system. For example, structure, interface and communication mechanisms function as architecture. Functional views can also describe the architecture. The following views illustrate the implementation details of the Oracle KYC architecture:

- **OFSAAI View**: Illustrates system components and their dependencies.
- **Deployment View**: Illustrates the deployment of components to processing nodes.

OFSAAI Architecture

The following figure illustrates the subsystems composing the OFSAAI architecture. These subsystems are used for application development and maintenance.
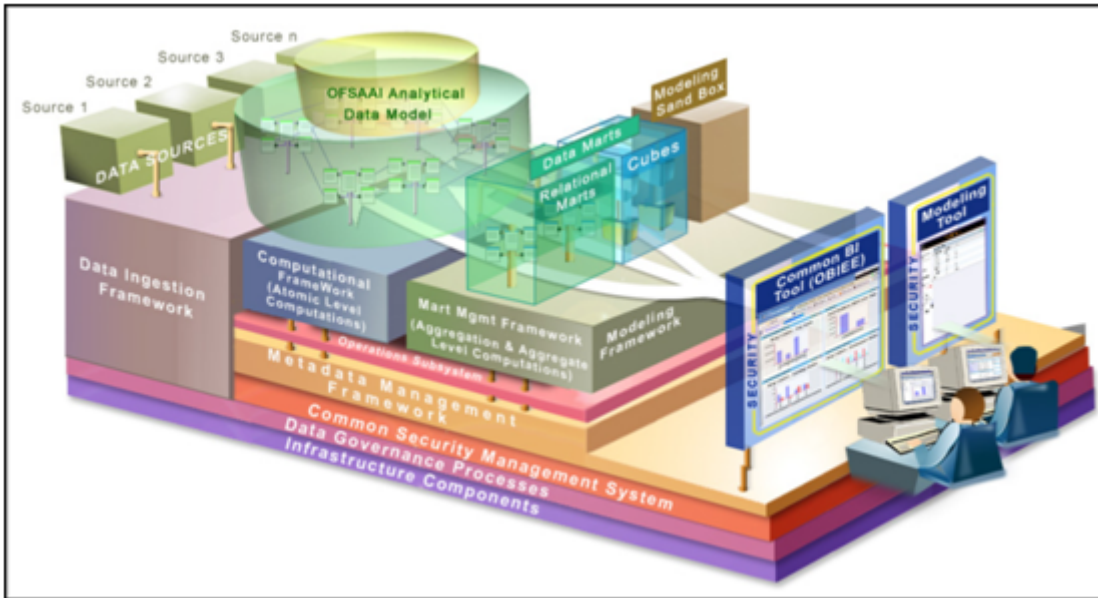
Figure 1. OFSAAI Architecture

The OFSAAI provides the framework for building applications, such as KYC. The deployment of multiple solutions and applications can occur on a single OFSAAI installation. Each adds domain-specific content to provide the required services for addressing a specific business problem. The OFSAAI includes reusable metadata artifacts and data structures. It also provides the required presentation packages and custom application objects for supporting the user interface functionality.
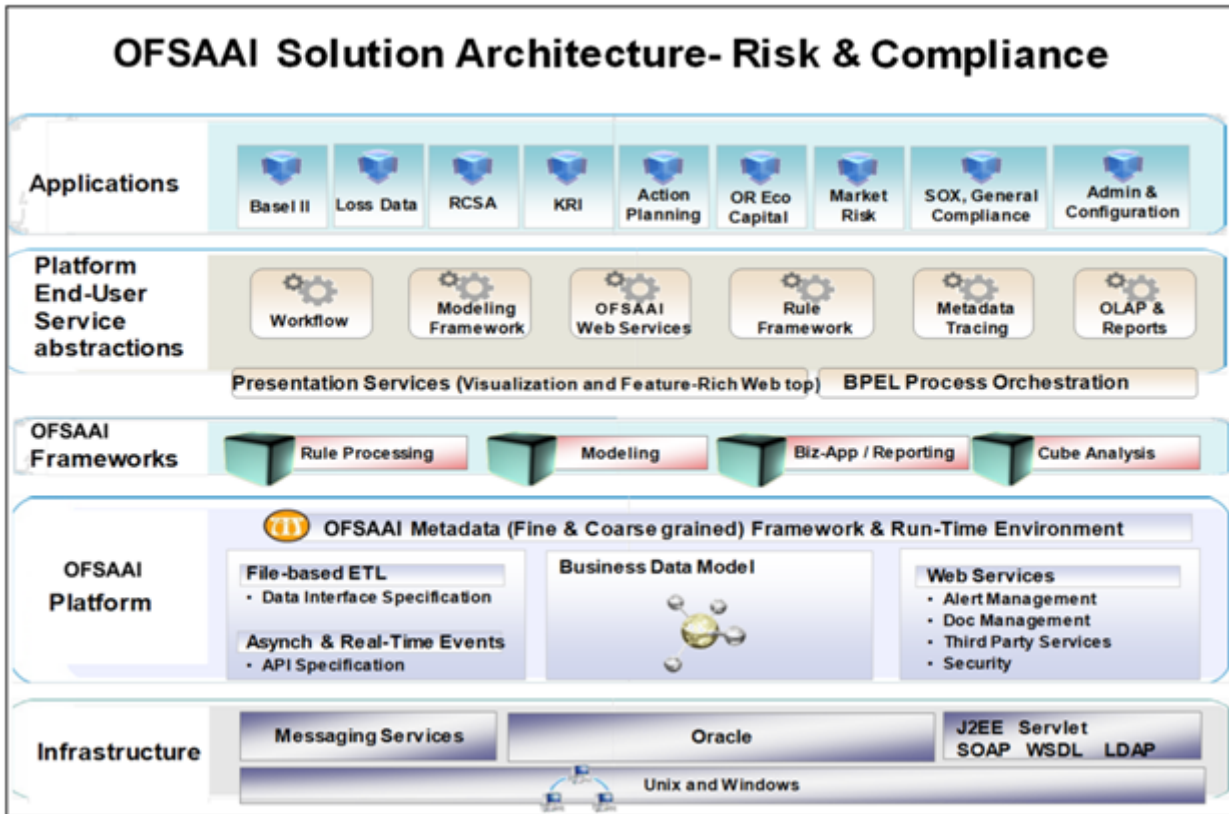
Figure 2. OFSAAI Solution Architecture

The following figure shows the primary communications links and protocols used between processing nodes.
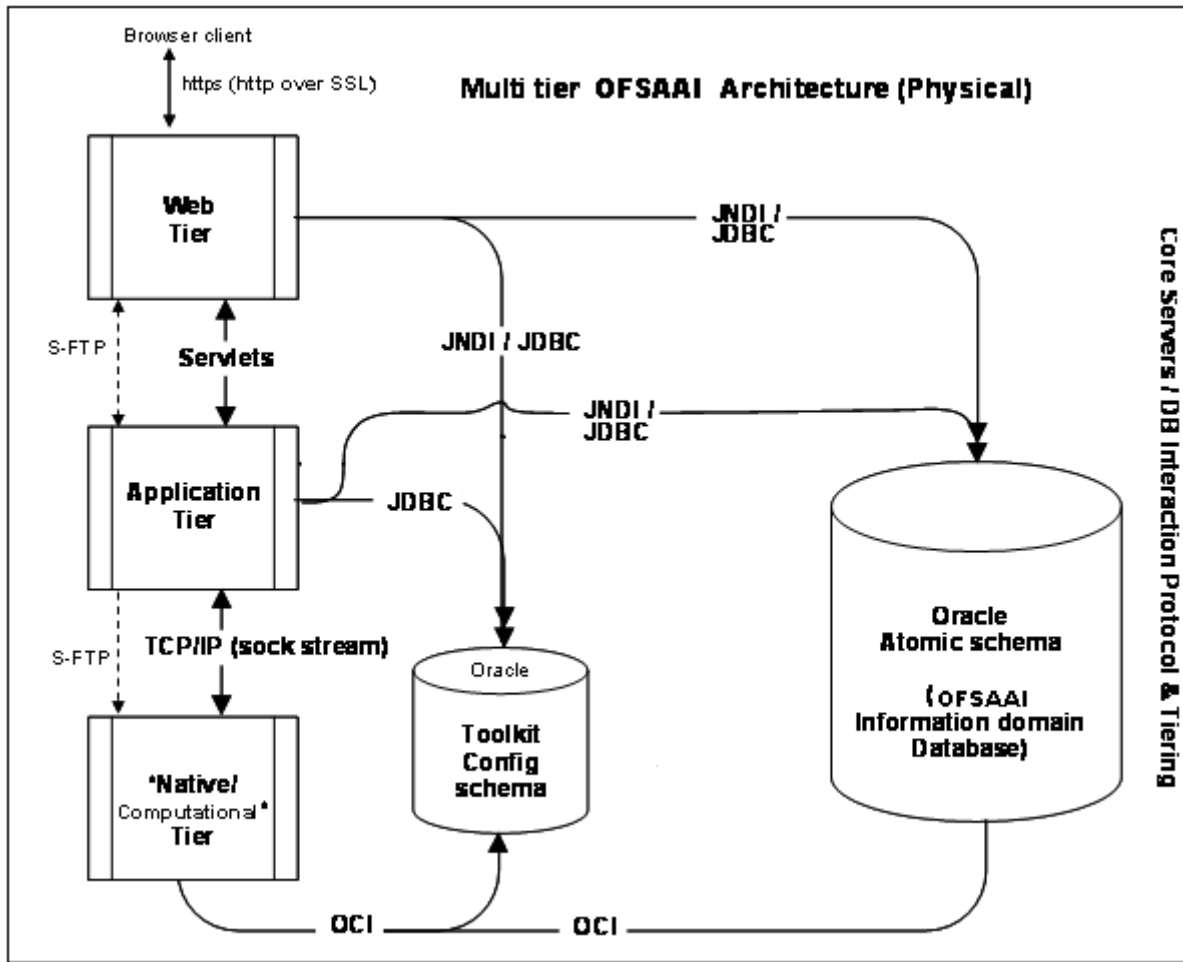
Figure 3. Communication Links and Protocols

Deployment View

The following figure illustrates the OFSAAI components when deployed on a single computer or when distributed across multiple computers:
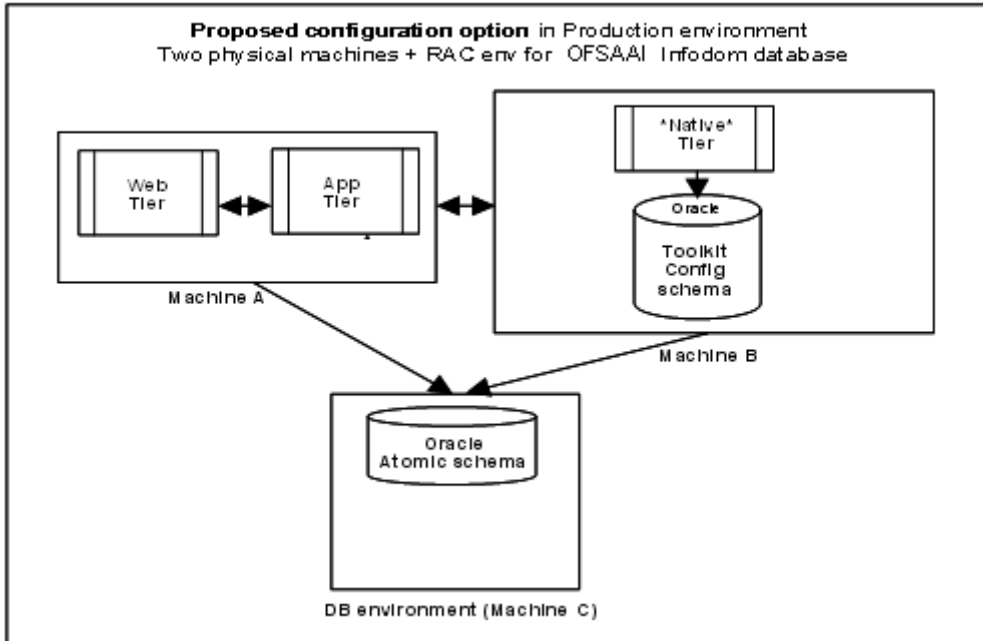
Figure 4. OFSAAI Components - Deployment Option A
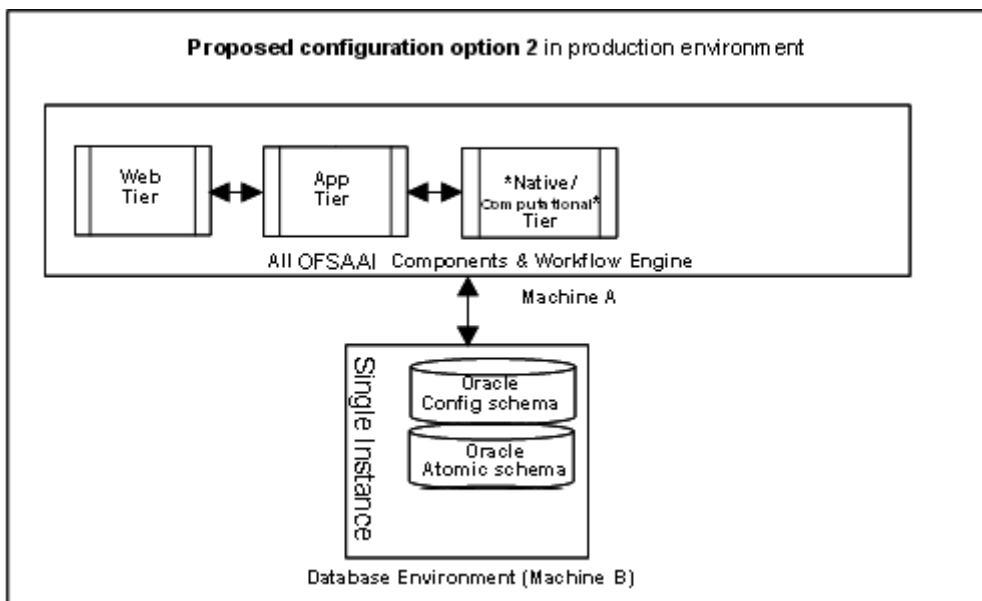
Figure 5. OFSAAI Components - Deployment Option B

CHAPTER 2 *KYC Operations*

This chapter discusses the following topics:

- Application Overview
- KYC Modules
- User Review
- Pre-requisites
- Operations
- Initial / One-time Activities
- Daily Activities
- Periodic Maintenance
- KYC Specific Terminology
- Real Time Account On-Boarding Review
- Regular Processing
- Risk Models
- End of Day Processing

Application Overview

Know Your Customer assesses the risk a customer poses to the bank or financial institution. It is not a one-time assessment, but is a continuous process of assessing customers. Customers are assessed in different stages of their relationship with the bank. The different stages of the relationship are described in the following sections:

- Deployment Initiation
- Real Time Account on Boarding
- Account on Boarding /Default Review
- Re-review

OFS - Know Your Customer – Application Overview
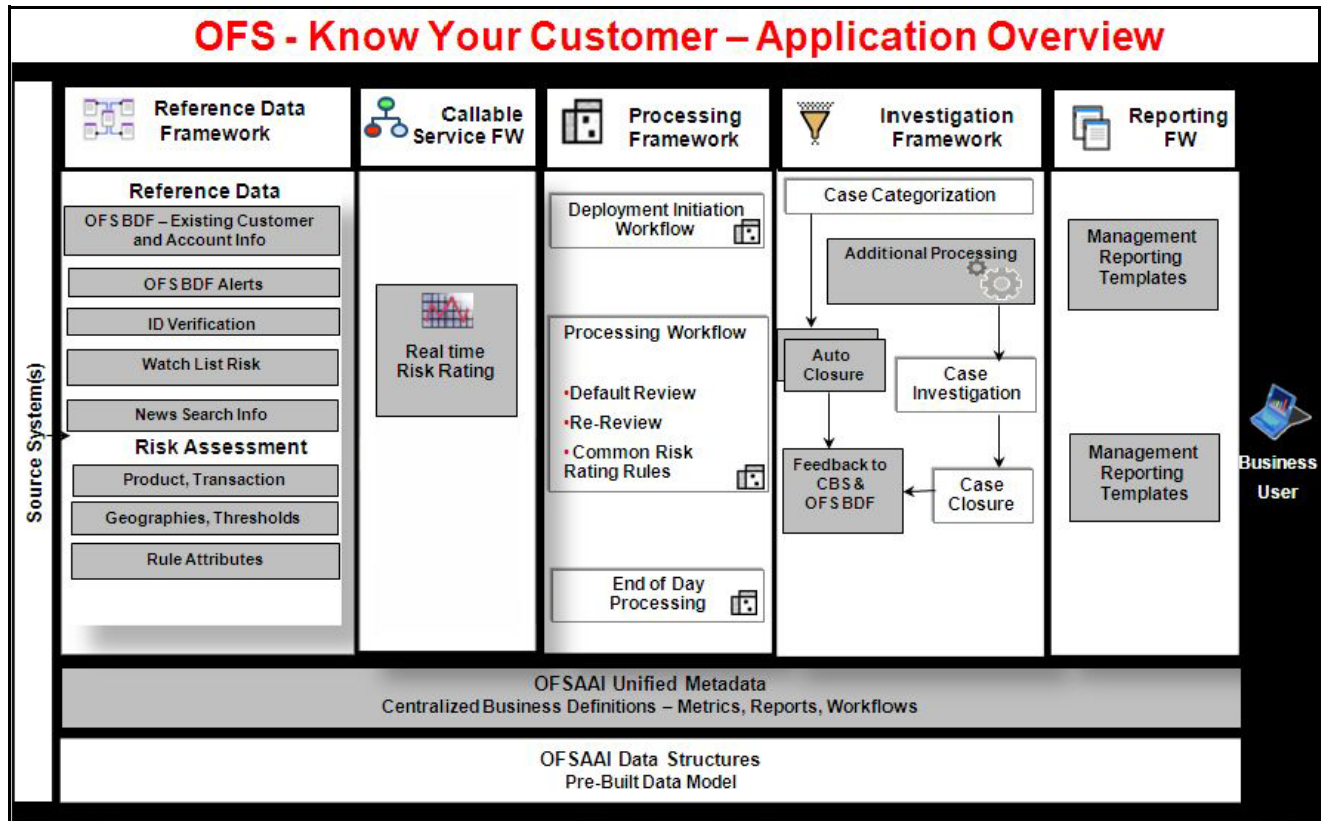
Figure 6. Know Your Customer Overview

The Oracle KYC, risk assessment application is built using the OFSAAI framework. The application functions are divided into the following areas:

- Reference Data Management (Internal and External)
- On-line interface with account opening system
- Risk Assessment Engine
- Interface with Third Party Services
- System Maintenance

KYC Modules

The following figure illustrates a High Level flow for the Real Time Review Process - Account Opening.
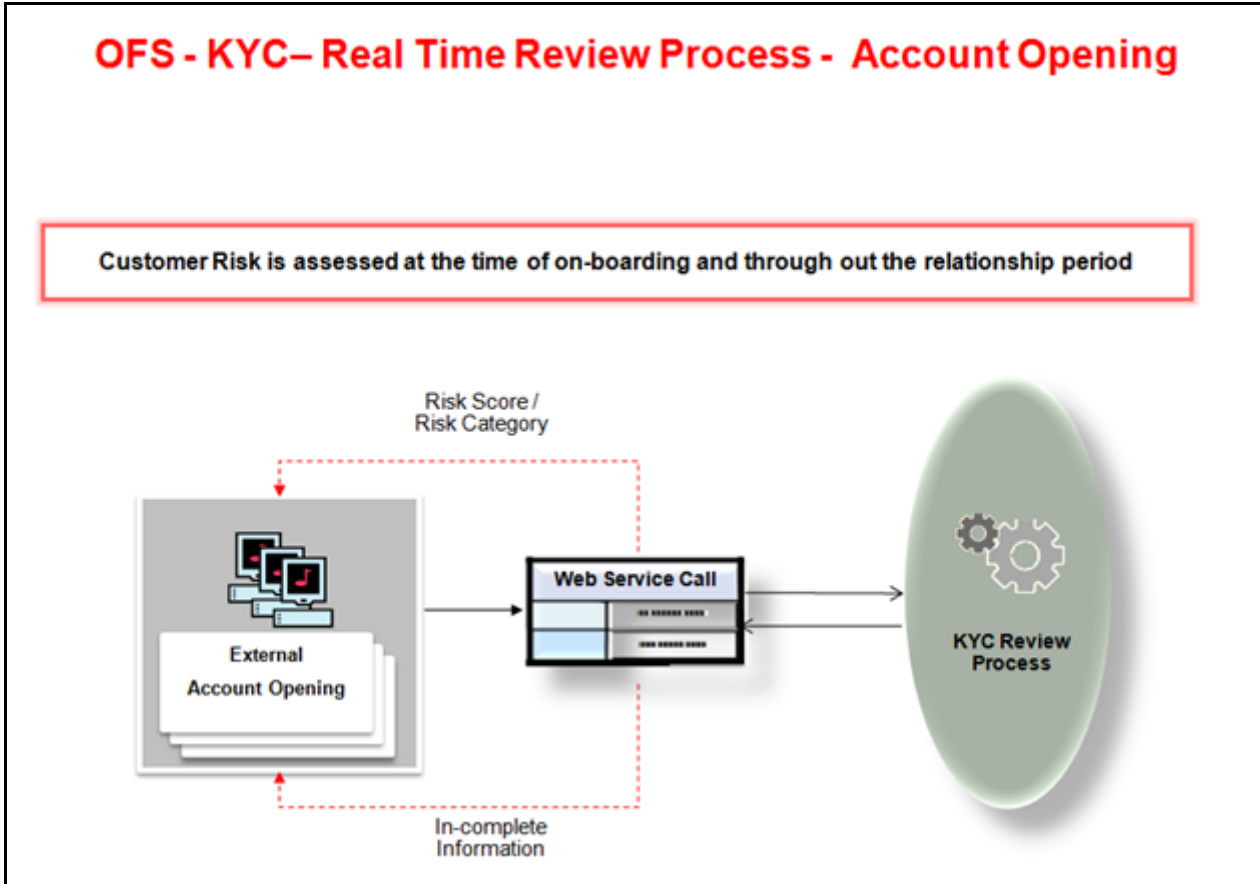
Figure 7. Review Process - Real Time Account On-boarding

The workflow steps may differ based on the type of review (default or re-review), but the Risk Assessment process is the same.

The following figure illustrates a high-level flow for default review and re-review processes:
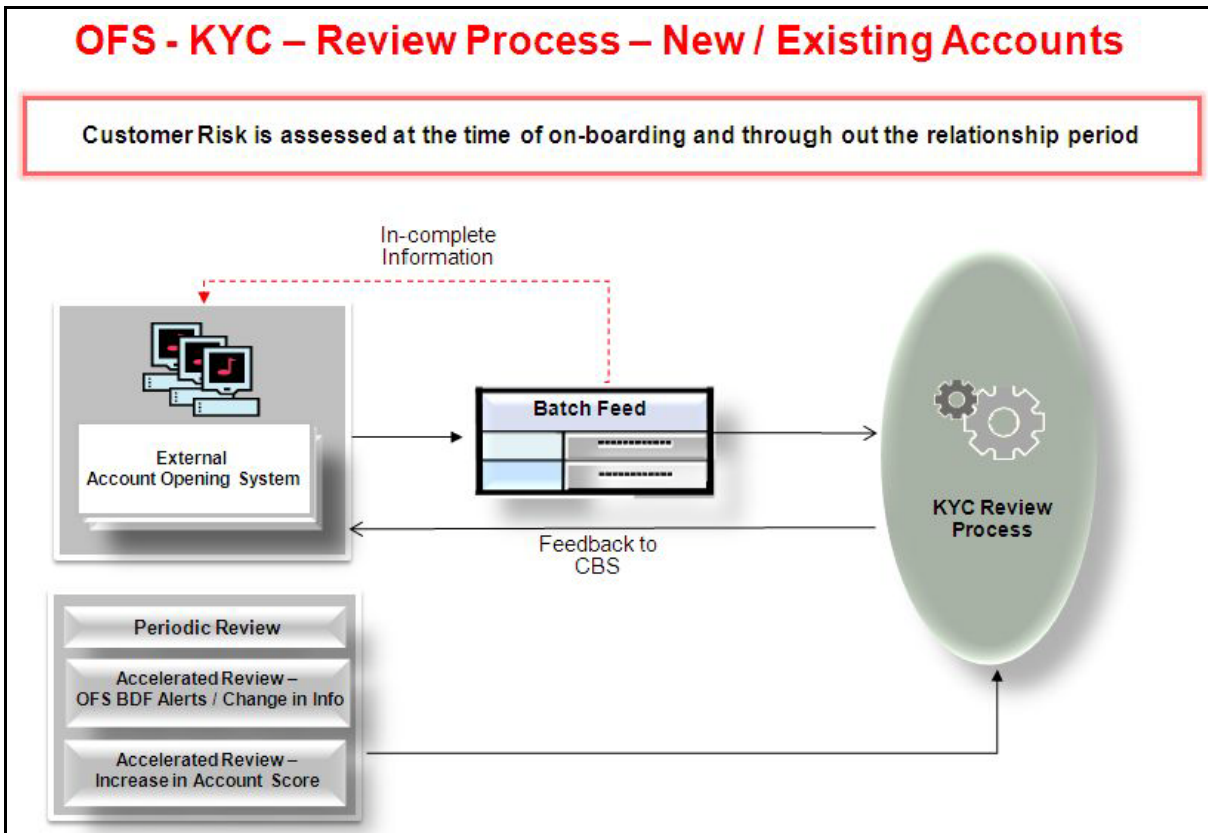
Figure 8. Review Process - New/Existing Accounts

The following figure illustrates a high-level flow for the default review workflow.
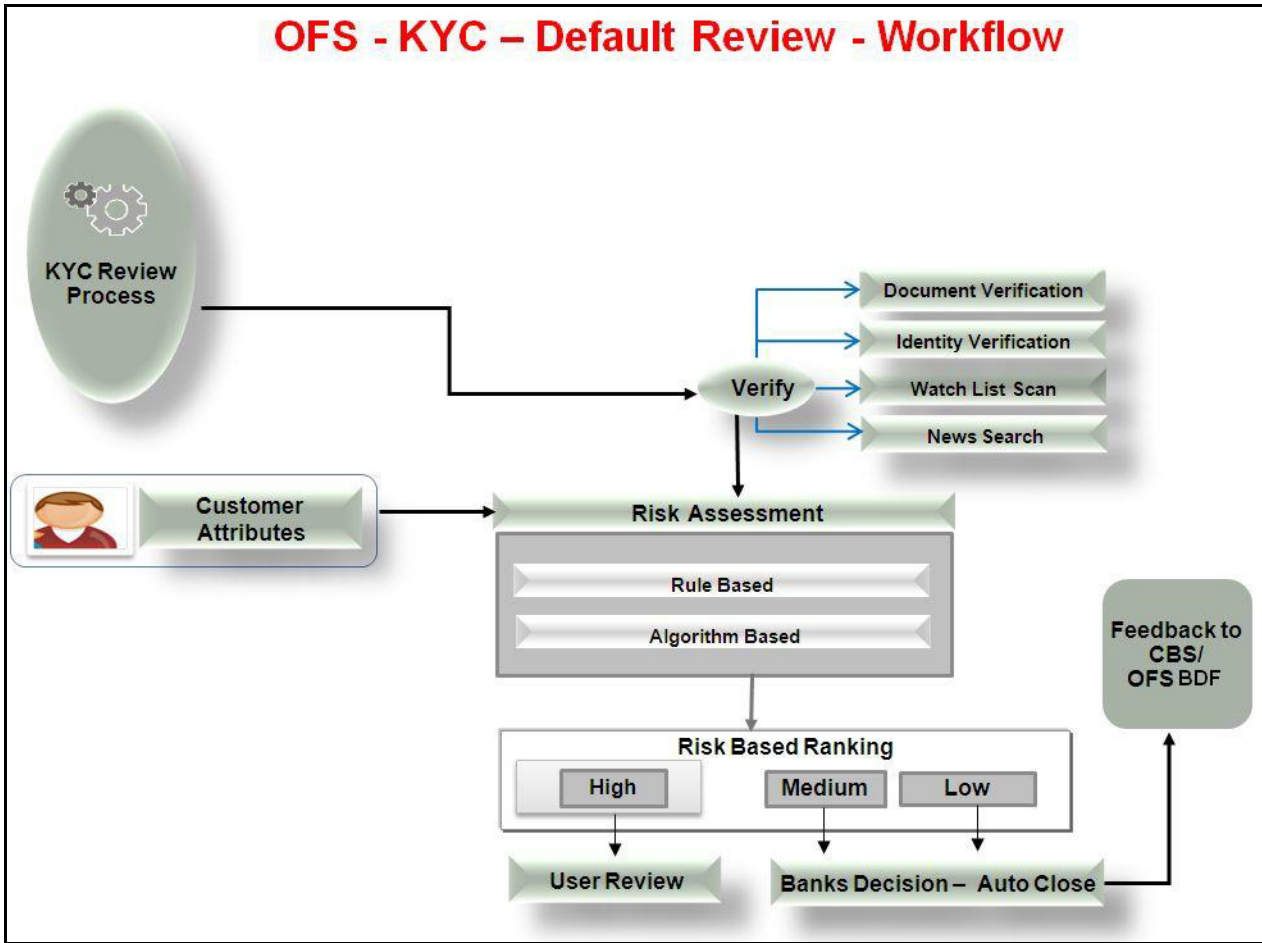
Figure 9. Regular Processing

The following figure illustrates a high-level flow for the re-review workflow:
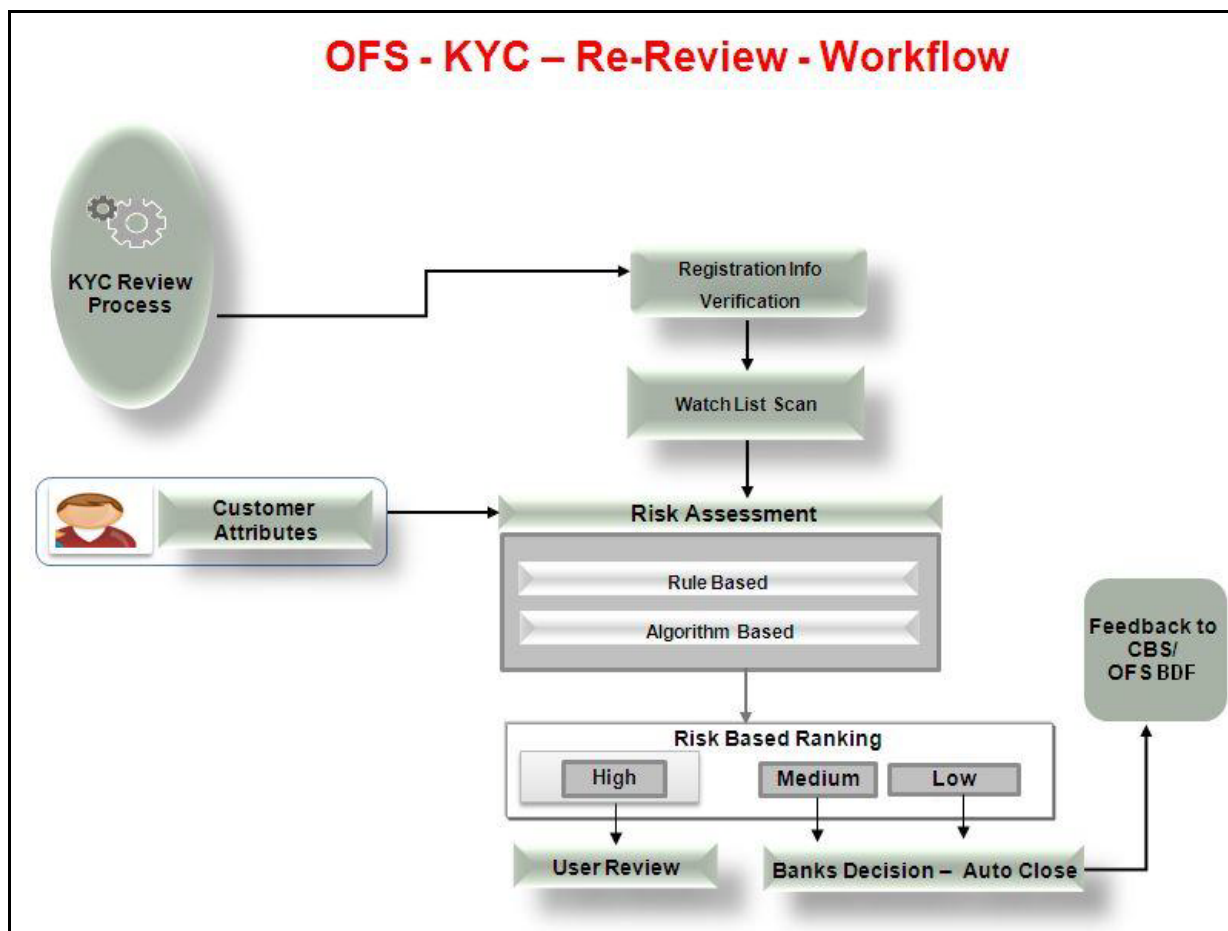
Figure 10. Re-Review Workflow

User Review

Risk assessments which are created by executing these workflows are categorized into Open Risk Assessments and Closed Risk Assessments once risk assessment process is complete.

Open risk assessments are promoted to cases in Oracle Financial Services Enterprise Case Management. Users can review these cases from the Oracle Financial Services Enterprise Case Management UI.

Risk Assessments which are not promoted to case are auto closed and the information is retained in KYC system.

Once the KYC case review is complete (Case Closure), feedback is sent to the Account Opening System and the Oracle Financial Services Alert Management system.

Case Closure is triggered through one of the following types of investigations defined in KYC:

- System Investigation (Auto Closure)

- User Investigation (Closed by the compliance user)

KYC assesses risk using the following processes:

- **Real Time Account On-Boarding Risk**: Risk assessment process at the time of account opening.

- **Deployment Initiation Workflow**: Risk assessment process for existing customers (One-time start-up activity) based on Jurisdiction, Customer Type and Length of Relationship.

- **Default Review**: Risk assessment of the newly opened account's owner.

- **Re-Review**: Periodic Review/Accelerated Review: Risk assessment of the customer. This process is based on Oracle Financial Services Behavior Detection Framework Alerts/Change in information.

- **User Review**: Risk assessment process (for both Existing and New customers) based on the case Risk Category.

Pre-requisites

The following pre-requisite activities must be completed before the OFS KYC configuration and maintenance begins:

- Installation of the OFSAAI using the OFSAAI Installer and OFSAAI Installation Manual

- OFSAAI Servers Start-up

- OFS KYC Pre-Installation Activities

- Completion of OFS KYC Installation

- OFS KYC Post-Installation Activities

Operations

Oracle Financial Services KYC operations are classified into the following types:

- Initial / One time Activities

- Daily Activities

- Periodic Maintenance Activities

Initial / One time Activities

- Managing Users

- Excel Upload Process

- Configuring Application Parameters

- Configuring Application Installation Parameters

- Configuring Rule Based Risk parameters

- Configuring Algorithm Based Risk parameters

- Defining Re-Review / Risk Thresholds

- Defining of Parameters used in the KYC risk assessment

- Setting up Document Guidelines

- E-Funds / Factiva Specific - Pre-requisites

- Setting up KYC Real-Time Service Request

- Scheduling of KYC batches

- Listing Holidays in the OFSAAI Administration User Interface.

- Deploying Initiation processing based on the implementation need.

Daily Activities

- Real-Time Account On-Boarding Risk Assessment

- Regular Processing Default Review

- Account Opening/Default Review System for the new accounts

- Accelerating Review Processing (after Oracle Financial Services Behavior Detection Framework alerts are created for the day)

- Re-Review / Periodic Review Processing

- Feedback / Application EOD Processing

- Configuration required for execution of batch

Periodic Maintenance Activities

- Clearing Staging Tables and Log Tables.

- Clearing of the log files related to previous batch executions.

- List Of Holidays

- KYC Purging Utility

Initial / One-time Activities

The following sections describe the Initial/One-time Activities.

Managing Users

KYC Administrator user has to be created for KYC related processing.

For more information on how to create users, refer to the *OFSAAI System Configuration & Administration User Manual* and *Configuration Guide*.

Excel Upload Process

The Excel upload process inserts the data into the appropriate dimension tables based on the pre-configured Excel upload definitions installed as part of the application installation. The Excel upload process will fail if there are primary key violations at the time of upload.

When uploading additional parameter values and associated risks, only the incremental records should be maintained in the Excel template with the correct unique identifier key.

The data in the Excel templates may refer to the data directly and the codes that are used to reference the data in a different dimension table. Referring to the incorrect reference code will lead to an unsuccessful upload process.

While populating data into `Dim_Jurisdiction` table through the Excel Upload activity, note that jurisdiction D is to be retained. D(Default) code is to be retained as it contains Default values which is required for risk processing if the data is not provided.

Note:

- In order to enable or disable accelerated re-review rules, the admin can modify the value of the column `F_ENABLE` in the excel sheet `VW_APPLN_REREVIEW_PARAMS` to Y or N respectively. Then the admin can proceed with the excel upload process.

- Jurisdiction codes in KYC 2.0 should match with jurisdiction codes in kdd jurisdiction table in alert management schema.

Data should be uploaded into the tables in the order mentioned in Appendix B, *Excel Upload Templates*, on page 51.

Configuring Application Parameters

Initially, the default values for the application parameters are to be populated into the database (DB) during Excel upload. The parameter values can be modified in the Excel data files before the upload process is done. This can be fine tuned through the User Interface provided by logging into the system as the KYC Administrator. The entries in the Application Parameters (`Appln_Params`) are used to control the flow of the application. These parameters are Jurisdiction-specific and must be populated for each jurisdiction in the `Vw_Appln_Params` table.

The values of these parameters will have an impact on the various services invoked by the solution, and the work flow of the solution. Multiple entries can be made for each parameter, one for each jurisdiction. It is mandatory that one set of parameters is present in the Application Parameters for the Jurisdiction *DEFAULT* which is pre-packaged and installed as part of application installation. For more information on how to navigate the UI and populate values for all jurisdictions, refer to the *Configuration Guide*.

Configuring Application Installation Parameters

The values for the Application Installation Parameters are to be populated into the DB during Excel upload. The parameter values can be modified in the Excel data files before the upload process is complete, or can be fine tuned through the UI by the KYC Administrator.

The Application Installation Parameters contain information about installation specific parameters which do not vary with the jurisdiction. This table has only one set of parameters for a particular installation. For more information, refer to the *Configuration Guide*.

Configuring Rule Based Risk Parameters

The default values for the Rule Based Risk Assessment Parameters are populated into the DB during Excel upload. Parameters and Values for the *DEFAULT* jurisdiction are provided in the Excel data file. The parameters are predefined and new parameters cannot be added. However, new values can be added for the parameters in the Excel data files before the upload process is complete, or new values can be added and modified from the UI.

Rule Based Risk Assessment Parameters contains information about the values for parameters which are pre-defined and the values for the parameters can vary according to the jurisdiction. It is mandatory to update values for the rules for all the jurisdictions for which Rule Based Risk Assessment is used.

Defining the Re-Review Risk Thresholds

Default values for the Re-Review Parameters are included as a part of the Excel upload. This section describes the Application Re-Review Parameters (`Appln_ReReview_Params` and `Vw_ Appln_ReReview_Params`).

The OFS KYC comes with pre-packaged rules based on which the Accelerated Re-Review is triggered. These rules are available in the Application Re-Review Parameters Table (`Appln_ReReview_Params`). All these 13 rules should be updated for each jurisdiction in the Vw_ Appln_ReReview_Params table. Each record contains a rule number with which it is associated in the Re-Review Processing Batch. Each rule can be enabled or disabled depending on the site-specific requirement. This table specifies details such as Look Back Period, Count of Alerts, and Alert Score for the Rule.

For more information, refer to the *Configuration Guide*.

Configuring Algorithm Based Risk Parameters

Default weights for each parameter of the Model-Based Risk Assessment Parameters are populated into the `Appln_Risk_Rating_Params` table in the DB during Excel upload. It is mandatory that one set of parameters is present in the `Vw_Appln_Risk_Rating_Params` table for the Jurisdiction *DEFAULT*, which is pre-packaged and installed as part of application installation.

The `Appln_Risk_Rating_Params` has 62 entries by default. The Risk Model Code and Risk Parameter Code columns indicate the model and purpose of each parameter. The `Appln_Risk_Rating_Params` table maintains the weight for each of the Risk Models/Risk Parameters.

Multiple entries can be made for each parameter, one for each jurisdiction, to support multiple jurisdictions in a single installation. Jurisdiction-specific parameters are available in the `Vw_Appln_Risk_Rating_Params` table. It is mandatory that all parameters are populated in the `Vw_Appln_Risk_Rating_Params` table for each jurisdiction specified in the `Dim_Jurisdiction` table. The pre-configured values can be fine tuned to suit the site specific requirements in the Excel data files before the Excel upload or modifying the parameter values after the Excel upload process by the KYC Administrator. For more information, refer to the *Configuration Guide*.

Defining Score for Values in KYC Risk Assessment

Risk values related to risk parameters are maintained in individual dimension tables. Data is populated into the dimension tables through the Excel upload to ensure successful execution of KYC batches. The data and risk scores must be fine tuned to suit implementation-specific needs.

Risk scores related to the static data in the respective dimension tables are used in risk score calculation. The Excel templates contain pre-configured risk parameter values and associated risk scores. These risk parameters can be

fine-tuned in the Excel data files before the data is uploaded or the value can be changed by the KYC Administrator. For more information, refer to the *Configuration Guide*.

Refer to *Excel Upload Templates,* on page 51 for more information about the upload sequence. These Excel templates are available in the following area:
`/ftpshare/STAGE/Excelupload/ KYCLookupTables>>` in the ficapp layer.

Setting up Document Guidelines

The internal document verification process happens before the external identity verification is triggered to collect data for the risk assessment process. The guidelines for verification should be set up as a start-up activity.

The guidelines must be entered in the Excel template available at
`/ftpshare/STAGE/ExcelUpload/KYCLookupTables/ FCT_DOCS_GUIDELINES.XLS` in the ficapp layer.

Upload the details through the Excel upload activity.

E-Funds / Factiva Specific - Pre-requisites

Oracle Financial Services Know Your Customer is integrated with external third party services for enhanced due diligence. KYC is also integrated with E-Funds for Identity Verification. The KYC Administrator can update the required configuration for identity verification from the UI.

KYC is integrated with Factiva for Negative News Search. The KYC Administrator can update the required configuration for identity verification from the UI.

For more information, refer to the *Configuration Guide*.

Setting up KYC Real-Time Service Request

KYC has a feature called Real-Time Account On-Boarding Risk (RAOR). This captures the details of a customer and interested parties during the time of account opening and calculates the risk of that customer.

Update the `KYC_XSD_LOC` parameter in the `APPLN_INSTALL_PARAMS` table through the Configuration option. This parameter specifies the path of XSD files which are required for the application.

Scheduling KYC Batches

The batches will not be visible in the Batch execution screen after the KYC installation is complete.

After the installation is complete, the user should login to the OFS KYC as the KYC Administrator and perform the steps mentioned in *Resaving Runs,* on page 63.

Table 2. Scheduling Batches

Criteria	Remarks
Timing of Execution of KYC batches	The KYC batches should be executed only after Oracle Financial Services Alert Management System has completed the day's ingestion and alert generation process. This ensures that the KYC will have the latest customer/account and alert information available for Risk Assessment reference. All the processing batches are EOD processing. The default review execution should be scheduled as an EOD activity.
Sequence of Execution of KYC batches	The Processing of batch should follow the sequence: • Deployment Initiation Processing - For processing the Existing customers • EOD Processing (Feedback Processing) - For processing after the entire DI processing batch is complete • Regular Processing - For daily processing. The feedback processing creates feeds for the account opening system and Oracle Financial Services Alert Management system. Care should be taken to ensure that the feeds are scheduled as part of the data ingestion process in the account opening system and Oracle Financial Services Behavior Detection Platform.

Listing Holidays in the OFSAAI Administration User Interface

Use the OFSAAI Administration UI (Administration>Security Management>System Administrator >Holiday Maintenance) to setup and maintain the holiday list for the financial institution.

Deployment Initiation Processing Based on the Implementation Requirement

After installing KYC, the existing customers are to be risk assessed and processed through KYC for which Deployment Initiation is required. The Deployment Initiation Process helps the financial institution process the risk assessment of an existing customer once as a start-up process and mark them for periodic review based on the CER score.

Deployment Initiation Processing can be done in a single slot or can be executed in multiple slots (for example, Number of Customers to be processed) for managing the performance due to volume. The pre-requisite for triggering the process execution involves setting up the KYC related parameters correctly using the application parameter configuration UI.

Refer to *Deployment-Initiation-Processing*, on page 47 for more information about the tasks within the Deployment Initiation processing batch.

Daily Activities

Before starting the daily processing activities, the processing date must be verified in the system using the Application Parameters screen under the KYC Administration option in the UI for the parameter KYC_PROCESSING_DATE. For more information, refer to the *Enterprise Case Management User Guide.*

Real-Time Account On-Boarding Risk Assessment

Processing the online request from the Account On-Boarding system assists in the account opening process.

The Real Time Account On-Boarding Risk Assessment (RAOR) workflow is triggered by the request from the external account opening system.This returns a risk score to the external account opening system. The request and response is sent as a Web Service Request.

Regular Processing -Account Opening Review

Data for the Account Opening Review System is picked from the ECM application database.

All the accounts which were opened the previous x days and are in *Active* status will be picked for risk assessment. The accounts which were opened in the last 7 days and activated the previous day will also be selected. The look back period is set to 7 days by default, but the value can be modified based on the requirement. The Account Range for Regular Processing parameter can be modified from the Application Parameters UI screen under the KYC Administration option by the KYC Administrator. For more information, refer to the *Enterprise Case Management User Guide.*

Regular Processing- Accelerated Review

Accelerated Review depends on the alerts generated by the Oracle Financial Services Alert Management system at EOD or due to changes in customer and account information. The Accelerated Review Processing is executed, along with Default /Account Opening review, after the Oracle Financial Services Behavior Detection Framework alert generation is complete.

Accelerated Re-Review has eight rules. Each of these rules checks for deviation from the standard for the customer. A case is initiated against the concerned customers if obtained values exceed the specified thresholds. The threshold values are stored in the Appln_ReReview_Params table under the following columns:

- Look back period
- Count of Alerts
- Alert Score
- Count of Changes

If the threshold is breached, a reason will be created in the Re-Review Case Reasons table (Fct_Rereview_ Ra_Reasons) for the creation of a risk assessment.

Regular Processing - Re-Review / Periodic

After every review (Account Opening Review / Deployment Initiation / Accelerated Review), the next review date is set for the customer based on the risk assessed. Thus, customers are periodically subjected to Risk Assessment, which is essential as the risk associated with each customer may change over time.

After a case is closed, the customer's next review date is determined by adding the time period (specified for the current risk category of the case) to the processing date in line with the holiday list definition.

Re-Review Processing checks whether the Next Re-Review Date in the Master Customer table matches the processing date.

A Risk Assessment is created for customers whose next review date matches with the current day's processing date. This batch is executed once every day.

Feedback/Application EOD Processing

During the execution of the regular processing batches, the risk scores at customer levels are sent to the Oracle Financial Services Alert Management system and the account opening system. The feedback batch achieves this goal by consolidating customers and their risk scores on whom the risk assessment was created, analyzed, and closed for the processing date.

The application also creates a KYC watch list feed for the Oracle Financial Services Alert Management system for the customers whose review is completed.

In addition, the second-level application staging tables maintained are cleared as part of the application EOD processing.

Periodic Maintenance

Clearing Staging Tables Log Tables and Log Files

Staging tables are populated during the Real Time Account On-boarding risk assessment process. The data must be cleared periodically for better DB space management. This facility is not pre-configured and is done as an implementation activity based on the implementation-specific requirements. For information on where the logs are created, refer to *KYC Batch Execution Logs,* on page 67.

Log tables can be cleared on a regular basis or as-needed by the client. The directory containing the log files should also be cleared on a regular basis.

List of Holidays

The bank is expected to update the list of holidays to the master Holiday List table.

To update the holiday list, follow these steps:

1. In the LHS menu of OFSAAI, select the KYC Infodom from the Connected to dropdown.

2. Navigate to Administration > Security Management. The OFSAA Infrastructure Administration page displays.

3. In LHS menu of Administration, navigate to System Administrator > Holiday Maintenance. The Holiday Maintenance page displays.

4. Click on the **Add** icon. The New Holiday pop-up displays.

5. In the New Holiday pop-up, click on the calender icon and select a date.

6. Click **Save**. The Holiday List updates and the selected date displays in the list.

To delete a holiday, follow these steps:

1. In the Holiday Maintenance page, select a date from the Holiday List.

2. Click the **Delete** icon. A message *Do you want to delete the holidays* displays.

3. Click **OK**. A message H*olidays deleted successfully* displays.

4. Click **OK**. The updated Holiday List displays.

The holiday list should be same in both Behaviour Detection Framework and KYC. The list of holidays should contain the weekly holidays as well as the annual holidays. Entries should be made well before the end of the calendar year, since this list is used by the OFS KYC to arrive at the Next Re-Review Date.

KYC Purging Utility

KYC data structures are populated through the workflows, such as Default Review, Accelerated Review, Re-Review Processing, Deployment Initiation Processing, Feedback Processing, and so on. Over a period of time, this data volume will grow and the application administrator should purge data from the production systems after the necessary archival process is completed.

This utility helps the application administrator purge the data from the Staging, Risk Assessment and Log tables.

KYC Specific Terminology

Customers

For more information, refer to the *KYC Risk Assessment Guide*.

Catch-All Bucket

In each of the Dimension tables, an additional entry is specified whose key is maintained as -999. This entry is also referred to as the catch-all bucket. If the customer provides data for a corresponding risk score that is non-existent in the Dimension tables, then the risk score of the catch-all bucket is used in the risk assessment process. By default, the risk score of the catch-all bucket is maintained at the highest value to denote a high-risk potential.

Auto Closure

Auto-Closure is based on the following criteria:

- The User Review Flag of the risk category to which the risk score belongs should be set to N.
- The difference between the present risk score and previous risk score should be less than the value specified in the parameter KYC_CHG_IN_CUST_RSK_TOLERANCE.

The Auto Closure process consists of the following steps:

1. In the Watch List Result table, update the High Risk Watch List Flag of the Case, if any such entry exists.

2. Update the risk scores and risk category into the Customer Master Table for the risk assessed customer.

3. Update the risk assessment ID from which the risk scores have been updated into the Customer Master table.

4. Determine the Next Re-Review date for the customer based on the risk category.

5. The risk assessments that are not auto-closed are promoted to case for further investigation.

Lookback Period

During Accelerated Re-Review processing for certain rules, the lookback period is specified. The lookback period is the time period within which the OFS KYC can consider the alerts in the Alert table (KDD_REVIEW in the Mantas schema).

For example, if the lookback period is set to 90 days for a rule, then during execution, the solution will look back up to 90 days to determine the list of alerts and to generate risk assessment reasons.

Real Time Account On-Boarding Review

The Real Time Account On-Boarding Risk Assessment (RAOR) workflow is triggered by a request from an external account opening system. The request format should be a Web Service Request.

Process Flow - Request and Response - Web Service

A third-party account service calls KYC Service on account opening and waits for a response. Each Real Time Request contains only the account opening information for one account per request. If the customer opens a savings and a checking account, the account opening system should send two requests to KYC for RAOR processing: one for the savings account and one for the checking account. A single request will not contain more than one customer's account opening details per request. Interested party definitions defined for the request will only be used for RAOR calculations.

The request generates the Request ID from the Sequence. The request ID and real time customer ID and account ID are stored in variables. This information is required to process the specific request through the following stages:

- Stage 1 - Acknowledgement Processing and RAOR Calculation - Pass 1

- Stage 2 - Third-Party Information Collection

- Stage 3 - RAOR Calculation - Pass 2

- Stage 4 - Send Acknowledgement

Stage 1 - Acknowledgement Processing & RAOR Calculation - Pass 1

The following steps should be handled in Task 1.

- Init Check

- Existing Customer - Real Time Customer Risk Assessment Processing

This registers the request and the Request ID, Customer ID and Account ID, which are the factors that uniquely identify the request. The requested XML is parsed and data is inserted along with the Request ID in respective Staging tables. Data is dumped into the following staging tables:

- Fct_Customers_Stg

- Fct_Cust_Addresses_Stg

- Fct_Cust_Phones_Stg

- Fct_Cust_Relationships_Stg

- Fct_Accounts_Stg

- Fct_Acct_Cust_Roles_Stg

- Fct_Cust_Country_Stg

- `Fct_Cust_Source_Wlth_Dtls_Stg`
- `Fct_Markets_Served_Stg`
- `Fct_Products_Served_Stg`

KYC Request Acknowledgement

Acknowledgement details should be stored in the DB for communicating the acknowledgement to the external third-party account opening system.

- A negative acknowledgement with error information is sent if any of the following situations is encountered:
  - If the user name or password is incorrect.
  - If mandatory information is missing.
  - If a request contains an account with different Primary Customer Definitions (Check against the Acknowledgement table).

In the above situation, there is no need for an error code or error message. The Flag(s) will be interpreted by the account opening system.

This checking is done on the data available in the staging tables for a specific Request ID and Customer Number. Other information is optional. Lack of availability will lead to dynamic weight calculation in risk assessment or non-availability in the UI display.

The system records the acknowledgement details in the `FCT_REQUEST_ACK_DTLS` table and also records the request in `CUSTRVWDTLS` and `ACCTRVWDTLS` tables if the customer is not an existing customer.

In the RAOR Pass 1 calculation, if the customer is an existing customer, the system performs the risk assessment calculation based on the Customer Type. For existing customers, RAOR PASS2 is skipped.

- **Legal Entity:** Updates the acknowledgement with CER and CER Category.
- **Correspondent Bank**: Updates the acknowledgement with CER and CER Category.
- **Individual:** Finds all joint customers defined in the request. If all of them are existing, then finds the max CER and updates the acknowledgement with CER and CER Category. Related updates are made in the Risk Assessment Summary and Risk Assessment Reasons tables.

Stage 2 - Third-Party Information Collection

IDV and Watch Lists are initiated for the customer and the interested parties defined in the request.

IDV is triggered only when the Doc Verification Flag is N or Null for the customer and interested parties and only when there is no prior result available in the IDV results table. WLS will be triggered for the customer and interested parties for every request even if the customer is opening more than one account on the same processing day.

Interested Parties of the customer definition in the context of RAOR processing:

- **Legal Entity:** Controlling
- **Correspondent Bank:** Controlling
- **Individual**: Only the New Joint Account Holders

Stage 3 - RAOR Calculation - Pass 2

If the RAOR Calculation is incomplete (customer is a new customer), then ROAR Risk Assessment is done based on the customer type. The related information is updated in the Risk Assessment Summary, Risk Assessment Reasons, Customer Review and Account Review tables.

Stage 4 - Send Acknowledgement

The system creates the return acknowledgement XML and returns to the Account On-Boarding System.

Regular Processing

The Default Account Review workflow should be triggered upon request from the following external account opening system:

The batch is split into the following sections:

- Accelerated Re-Review Reasons
- Customer Identification
    - New Customer Identification
    - Identifying the customers whose status are cleared from Hold
    - Identifying the customers based on accelerated re-review rules
    - Identifying the customers based on re-review date
- Risk Assessment Creation - Primary, Guardian/Joint Account Holders
- Master Customer and Account Table Maintenance
- Copy Snapshot - From Oracle Financial Services Behavior Detection Framework Bus Schema for all the risk assessments created
- Registration Information Flag and Request for Latest Information
- Watch List Scanning (Request / Response)
- Document Verification
- ID Verification (Request / Response)
- Negative News Search (Request / Response - Including the Documents)
- Risk Assessment Initiation
    - Rule-based Risk Assessment
    - Algorithm-based Risk Assessment
- Closure Updates
- Promote to Case
- Customer - Risk Assessment History population

The OFS KYC requires an online/batch interface to facilitate Watch List Scanning, Identity Verification, News Searches and so on for the successful execution of the default review

The Account Opening Review is executed at the end of the day and the results are computed.

There will be two ways to execute the batch for Account Opening

- Regular Processing on daily basis (Combined batch with Re-Review)

- Weekly Processing on weekly basis(Combined batch with Re-Review)

Accelerated Re-Review Reasons

There are 13 accelerated re-review rules that refer to the tables in Alert Management/ Business schema. These rules generate reasons which ultimately result in creation of risk assessments.

Accelerated Re-Review processing refers to generation of risk assessments based on alerts created by Oracle Financial Services Alert Management system. Periodic Re-Review processing refers to risk assessment of the customers already risk assessed after a gap of specified time period.

An Accelerated KYC Review is triggered based on behaviors detected in the Oracle Financial Services Behavior Detection Framework. Oracle Financial Services Behavior Detection Framework alert data is used to create a KYC risk assessment due to re-reviews rules. Re-Review rules processing is a batch activity. The batch is scheduled after the Oracle Financial Services Behavior Detection Framework alert generation and processing event. The Customer / Account Details will be referred from the Business schema and Alert details will be referred from the Alert Management schema. Re review rules are part of Regular Batch.

Customer Identification

For every customer who has an account in the bank a risk assessment is created. KYC solution identifies the customers who need to be processed for the creation of the Risk assessment as per the below conditions:

- Customer should be an active customer

- Customer should have at least one account mapped to him

- The account mapped to the customer should be an active account

- Customer should be having a controlling role on the account mapped to him

Interested parties are calculated for the customers who are identified for the Risk assessment creation and are stored in the KYC system.

Risk Assessment Creation

Risk Assessments are generated for the primary account holder's, joint account holders and guardians of the accounts for whom a positive acknowledgement has been generated. Each Risk Assessment is identified by the Risk Assessment reference associated with it. Risk Assessment reference is generated by appending the customer ID to the word 'CASE' and then appending the processing date (In YYYYMMDD format) to the result. This ensures that each risk assessment is unique. Only one Risk Assessment is generated on a customer per day (If the parameter- RA Periodicity is configured as one in Vw_Appln_Params table).

Risk Assessment Periodicity is another parameter considered while generating Risk Assessments. The value associated with this parameter defines the minimum duration between two Risk Assessments on the same customer.

Risk Assessment Periodicity can be fine-tuned further using the configurable parameter, depending on the implementation needs.

Refer to the parameter KYC_CASE_PERIODICITY_IN_DAYS in *Application Configuration using OFSAAI Configurability,* on page 57 for more information.

KYC Master Customer and Master Account Table Maintenance

When a new account is opened or a new customer joins the bank, in case of positive acknowledgement, a record is made in the respective KYC Master Customer and Account tables. The tables contain information related to previous and present risk calculation of the customer/account.

Copy Snapshot

After Risk Assessment creation, the KYC solution copies customer and account data as on Risk Assessment creation date into a new set of tables with each record tagged to the Risk assessment to which it belongs. The data is fetched from the business schema (ECM).

Registration Information Flag and Request for Latest Information

If the time period between the processing date and the last updated date of the customer's information is greater than the value specified in the application parameter Minimum Verification Time Period (KYC_MIN_VERF_TIME_PERIOD), then the risk assessment status is changed to HOLD. Subsequently, the Registration Information updation required Flag is set to Y in Fct_ra table. The risk assessments which are in HOLD status will be visible only to the user who is mapped to the Relationship manager role. When the relationship manager verifies the customer information and updates the risk assessments assigned to him as 'Verified - Entity Info is Recent' in the UI it will set the Registration Information updation required Flag back to N. Meaning the customer's information is updated and new set of data relevant to the risk assessment can be picked up from the Business schema. If the Relationship Manager verifies the customer information and finds that the information available is the latest, he will update the risk assessment as 'Verified - No change required' it will set the Registration Information updation required Flag to NA, then the old snapshot information is retained and used for further processing.

Note: The system assumes that the information has been updated in the source system.

Watch List Scanning

The risk assessed customers and interested parties are checked against a list of closely monitored individuals and entities by carrying out a Watch List scan. This is done to identify the existing and prospective customers whose names have already been put up on the Watch List. The OFAC result and score obtained as a part of Identity Verification are also used for Watch List Scanning. Currently, the solution has been configured to interact with the Oracle Financial Services Behavior Detection Framework Watch List. The third party service can also be modified to allow the solution to interact with any other Watch List as well. The application parameter Third Party Watch List Scan (KYC_TP_WL_SCN) is a part of the Watch List rule. This allows the customer to disable the rule if scanning is not desired.

Document Verification

After Risk assessment generation, the documents supplied by the risk assessed customer are verified to confirm the customer's identity. A list of documents is provided in Document Guidelines Table (Fct_Docs_Guidelines), along with the level to which they belong. A customer's identity is considered confirmed only if the required number of documents of desired level is provided. The number and level of the document can be configured by modifying the content of the parameter KYC_DOC_VERF_REQD in the Vw_Appn_Params table.

ID Verification

The customer type provided by the external Account opening system should match with the customer type provided in the KYC solution. If there is a mismatch in the customer type then risk assessment will not be created on the particular customer and hence risk assessment will not take place for that customer.

If the customer has not provided sufficient documents, the result of document verification is negative. Thus, to determine the identity of the customer, an external ID Verification is triggered. External Identity verification is triggered only when the internal system based document verification process is unsuccessful and there is no prior external identity verification done. Identity verification, when initiated, is done for the customer and customer's interested parties.

By default, the KYC solution is configured to available services of eFunds IDV search to confirm the customer's identity. The solution can be modified to interact with other service providers to carry out ID verification.

ID Verification can be switched on / off, in the KYC solution by altering the values of the parameter KYC_IDV_DEFAULT_SCORE. This parameter also provides the default score, for those customers for whom no IDV score was obtained.

Negative News Search

For all the risk assessments that have been created on the same day and are still in initiated status, the negative news search is initiated against the risk assessed customer and interested parties.

Currently, the KYC solution has been configured to interact with Factiva, a Negative News Search service provider. At the time of implementation, the Negative News Search service provider can be changed to any other entity.

The application parameter KYC_TP_NN_SCN is used during Negative News Search. This parameter contains all the details necessary to access the Factiva Web site. (OFSAAI -Oracle Financial Services KYC solution is pre-configured to interact with Factiva for Negative News Search).

Risk Assessment Initiation

Based on the reasons generated in the previous module, risk assessments are created for the corresponding customers. The type of risk assessment source is specified as *Accelerated Re-Review.*

Then the next Re-Review Date for each customer is compared to the day's processing date. If the two match, then a risk assessment is created for the customer with the risk assessment source specified as *Periodic Re-Review.*

Rule-based Risk Assessment

Rule-based assessment calculates a CER score based on client configurable rules. Rule-based assessment model is executed only if it is chosen by the bank or FI for an installation. This option can be decided using the Rule-based assessment parameter available in the jurisdiction-specific Application Parameters table. For more information about the Rule-based assessment model parameters, refer to the *Configuration Guide.*

Rule-based assessment model supports a business process framework, which allows the bank or FI to provide different values for the pre-defined rules. Once a customer is assessed using the Rule-based Assessment Model, they will not be assessed further using Algorithm-based Assessment Model.

For Rule-based assessment, the values for each rule are provided to the system through the KYC Configuration Rule Based Assessment Model User Interface by the Admin user. For more information about providing values for rule-based assessment, refer to the *Configuration Guide.* The bank or the FI can provide as many values as required for a rule.

A customer can fall under one or more rules during rule-based assessment. When a customer has been matched to multiple rules, the system considers the maximum score of the matched rules.

For example, a customer has matched the Country of Citizenship and Country of Residence rules, with the values being Afghanistan and India, with a score of 45 and 60 respectively. In this case, the system considers the CER as 60 for the customer. It also captures and display all the rules matched.

All risk assessments created using this work flow will be automatically promoted to a case irrespective of the CER score. This overrides the ranges defined in the Risk Category table User Review flag as *Y.*

Algorithm-based Risk Assessment

Customers who are not assessed using the Rule-based Assessment Model are assessed using Algorithm-based Assessment Model.

Algorithm-based Assessment Model calculates the risk of customers based on different parameters which are based on customer type.

For each parameter the system checks the value provided by the customer who is being risk assessed, and retrieves the score of that value from the respective static Jurisdiction table. If the value provided by the customer for a parameter is not available, then the system considers it as Others which would have a corresponding score in the static jurisdiction table. If the customer has not provided any value for a parameter then the system would go in for Dynamic weight to distribute the weight of this parameter across other parameters.

CER Score = Sum (value of the risk assessment parameter * weight)/100

Closure Updates

After Risk Assessment, some of the risk assessments are eligible for Auto Closure based on the following criteria:

- The User Review Flag of the risk category to which the risk score belongs should be set to N.

- The High Risk Watch List Flag of the Risk assessment should be set to N.

- The difference between the present risk score and previous risk score should be less than the value specified in the parameter KYC_CHG_IN_CUST_RSK_TOLERANCE.

For all the risk assessments that satisfy the above set of conditions, the records of the risk assessed customers in the KYC Master Customer Table (Fct_Cust_Rvwdtls), is updated with all the parameters pertaining to the risk score calculation. Subsequently, the records of all the accounts associated with the risk assessed customer are also updated

with the risk scores. The threshold values for Auto-Closure can be altered by changing the value of the Application parameter mentioned above.

Promote to Case

During Risk Assessment Promotion to Case, there are possibilities of few risk assessments not being promoted to case which can be because of non-availability of data, system issues, server problems etc.

The error for the Risk Assessment not being promoted to a case will be captured in the table RA_TO_CASE_ERROR. This table will be available in the KYC Atomic schema. The user should be able to identify the cause of the error and resolve the same. Once the error is rectified, these Risk Assessments will be promoted to a case during the next KYC batch processing.

Deployment Initiation - Processing

This batch is to be executed only once at the time the KYC solution goes live. All the sections listed under this batch are part of the Re-Review Processing Batch also. The batch is split into the following sections:

- Customer identification for Risk Assessment
- Tagging data to the cases
- Watch List scanning
- Risk Assessment
- Auto Closure
- Promote to Case
- Customer - Risk Assessment History population

Refer to the similar sections in Re-Review Processing for description of each of the sections. Risk assessment process for the existing customers is done based on the following:

- **Jurisdiction**: Oracle Financial Services client can process the deployment workflow based on specific jurisdiction.
- **Customer Type**: Oracle Financial Services client can also process the data based on customer type.
- **Length of Relationship**: Oracle Financial Services client can also process the data based on length of relationship of the customer and this is configurable.

Note: All the above criteria for processing can be done separately or by combining them.

Refer to the KYC_DEPLOYMNT_INIT_WF parameter under the application parameter.

Risk Assessment

For KYC Risk calculation, the following are required:

- Risk Assessment Models, Risk Assessment Model Parameters and their appropriate weights.
- For Every Risk Parameter, Possible Values and their Risk Score

- Customer Attributes for each of these risk parameters

This module represents the computational engine of the OFS KYC.

Risk Models

KYC risk models are of the below types:

- RAOR

- Rule Based

- Algorithm Based

For more details, refer to *the KYC Risk Assessment Guide.*

Catch-All Bucket in Dimension Tables

If the data provided in the fact tables does not match with any of the values in the dimension table, then the score associated with the default value specified in the dimension table is utilized. This default entry is identified by the name *Others* or the key '-999'.

Dynamic Weight Calculation

The overall weight of all the parameters is always equal to 100. During the Risk score calculation, the data provided for the customer is compared with the static data in the mapping jurisdiction tables and the relevant risk score is used. There are three possible scenarios as described below that can be encountered during the calculations:

- Data is available, but the equivalent entry is non-existent in the dimension mapping jurisdiction table. Here the default risk score stored in the 'Others' category is used for the calculation.

- Data is available and an equivalent entry is present in the dimension mapping jurisdiction table. The appropriate risk score is used in the calculation.

- Data is not available. As a result the risk score cannot be identified. As a result, dynamic weight calculation is used, to calculate the correct risk score.

Since the weight for a valid parameter is less than 100, the risk assessment engine increases the weight and the related risk scores that the newly calculated weight equals 100. This ensures that at the time of the risk assessment, the over-all weight for the valid parameters is always 100 and the risk score is proportionately incremented.

For more information, refer to *the KYC Risk Assessment Guide*

End of Day Processing

Feedback to the Oracle Financial Services Behavior Detection Framework / Account Opening System

At the end of each day, risk scores for risk assessments that are auto-closed or closed by the compliance officer after investigation are sent to Oracle Financial Services Behavior Detection Framework and the Account Opening System through Feedback files. Watch List files and Feedback files to the Account Opening System are available after KYC End of Day (EOD) processing is complete. These files must then be scheduled for loading into Oracle Financial Services Behavior Detection Framework and the Account Opening System. The processing date will be the date of KYC EOD Processing.

- CBS Feedback (incremental dump of processing day for Oracle Financial Services Alert Management system)

- Watch List Entry Feedback (full dump as of processing day)

- Customer - Risk Assessment Details (Incremental dump as of processing day for the Account Opening System) The delimiter for the extract file can be defined under Unified Metadata Data Integrator. Refer to the Appendix D, *Extraction Definition*, on page 59.

CBS Feedback

This file contains the Customer ID and the risk score computed by the risk assessment engine. The file name is obtained by appending the processing date to GenCustDetails_ED. The Feedback Flag will update in the FCT_CUST_RVWDTLS table. KYC will not send Customer Feedback unless the Business schema is present. This file will be sent in the batch which runs in the subsequent days.

Table 3. CBS Feedback

SL No.	Business Name	Data Type
1	Risk Assessment ID	String
2	Customer ID	String
3	Customer Name	String
4	Customer Effective Risk Score	Number
5	Risk Assessment Closed Date	Date
6	Next Re-review Date	Date

Watch List Entry Feedback

The Watch List is generated for closed cases and where closure is recommended for the Account. The records populated in the Watch List results table for a processing date are dumped into this file. The file name is obtained by appending the processing date to GenWLSFeedback_ED.

Table 4. Watch List Feedback

SL No.	Business Name	Data Type
1	Entity Identifier Type	String
2	Entity Identifier	String
3	Watch List Identifier(Referred from Application parameter KYC_WLS_ENTRY_FILE_ID)	String
4	Watch List Entry Description Text	String

Customer - Risk Assessment Details

This file contains the Customer ID and the Risk assessment details computed by the risk assessment engine. The file name is obtained by appending the processing date to GenCustDetails_ED. This file is created for the Alert Management System to verify the Risk assessment details which were Auto closed on that day during processing or UI Closed by the investigation officer.

Table 5. Risk Assessment Details

SL No.	Business Name	Data Type
1	Customer ID	String
2	Customer Effective Risk Score	Number
3	Custom1Date	String
4	Custom2Date	String
5	Custom3Date	String
6	Custom1Real	String
7	Custom2Real	String
8	Custom3Real	String
9	Custom1Text	String
10	Custom2Text	String
11	Custom3Text	String
12	Custom4Text	String
13	Custom5Text	String
14	Source System	String

Customer - Risk Assessment History

The KYC solution captures the history of all the risk assessments created on all the customers within a period of 12 months and would retain for x period of months. 12 months is configured by default, the administrator can update this parameter based on the client requirement. The value can be updated from the UI for the 'V_ATTRIBUTE1_VALUE' for the 'KYC_RISK_ASSESSMENT_HISTORY' parameter of the Application Install Parameters. A partition will be created on the table based on the value which is updated.

Incrementing the Processing Date

The KYC solution refers to the Application Parameter KYC_PROCESSING_DATE to pick up the date. At the end of each day, this date is set to the next working date.

Renaming and Transferring Feedback files

When a KYC review for a new account request is complete, KYC informs the Account On-Boarding System about the disposition of the review. At the disposition of a periodic or accelerated KYC review, the KYC system communicates the results of the review to the appropriate banking system used within the financial institution, such as an Account Management System. The parameters required for renaming and transferring feedback files should be configured in the appln_install_params.

The Oracle Financial Services KYC system is also responsible for sharing Account, Customer, and Watch List feedback to the Oracle Financial Services Alert Management system and Oracle Flexcube system at the disposition of the KYC review.

The extract names are not compatible with the Oracle Financial Services Behavior Detection Framework file naming convention. This utility will complete the following activities based on the configurations set for the implementation:

1. Moves the files to the different location in the same server.

2. Renames the files with the extension defined.

3. Maintain a copy of the extract in the history directory with its original name.

4. The utility covers the following extracts in KYC 2.0:

- GenCustDetails_ED<YYYYMMDD>

- GenWLSFeedback_ED<YYYYMMDD>

Utility for Periodic Review-Customer distribution

This utility distributes fixed number of customers into different Next Re-Review Dates so that huge number of Cases are not processed in Periodic Re-Review in a single day. This task is tagged in the EOD batch and to be executed after successful execution of deployment initiation batch.

The following parameters must be set for execution of the utility through the batch execution screen:

- Number of Customers per day.

- Number of days from when the customers need to be distributed.

These parameters must be set before running this utility.

Utility for Purging

KYC data structures are populated through Default Review Processing, Accelerated Review Processing, Re-Review Processing and Deployment Initiation Processing. Over a period of time, this data volume will grow and the application Administrator will need to purge data from the production systems after archiving.

This utility helps the application Administrator to purge data from the Risk Assessment tables based on the purge requirement.

Archival is not done by this utility. Required backup and archiving of the database and tables must be done outside this utility.

The utility will take *number of day*s as input for the retention period for the Auto closed risk assessments and the *number of days* as input for the retention period of the UI closed risk assessments. The administrator should update a whole number in the V_ATTRIBUTE2_VALUE and V_ATTRIBUTE5_VALUE respectively in the VW_APPLN_PARAMS table for the KYC_PURGE_ARCHIVE_PARAMTERS parameter.

The utility will also take the range of the CER score as another input during the purging of the risk assessments. The Administrator can update the minimum and maximum range of the CER score in the 'V_ATTRIBUTE3_VALUE' and 'V_ATTRIBUTE4_VALUE' columns of the VW_APPLN_PARAMS table for the KYC_PURGE_ARCHIVE_PARAMTERS' parameter.

Purge utility is defined as a data transformation in OFSAAI and it is a part of the EOD processing and the Regular Processing batches. The Purging of the Risk assessments can be done based on Jurisdiction also. *ALL* is configured by default as the jurisdiction parameter, the risk assessments related to all the jurisdictions will be purged by default. In order to purge only risk assessments related to a particular jurisdiction, the Administrator must update the specific jurisdiction code in the 'V_ATTRIBUTE1_VALUE' of the VW_APPLN_PARAMS table for the KYC_PURGE_ARCHIVE_PARAMTERS parameter.

Purging Risk Assessment Related Tables

Accept the number of days for the retention period and the risk range as parameter.

Delete the dependent records first and then the required records.

Delete data from the following tables that are older than the given date in the order specified below:

1. FCT_REREVIEW_RA_REASONS

2. FCT_RA_CUSTOMERS

3. FCT_RA_ACCOUNTS

4. FCT_RA_ACCT_CUST_ROLES

5. FCT_RA_CUST_RELATIONSHIPS

6. FCT_RA_CUST_ADDRESSES

7. FCT_RA_CUST_COUNTRY

8. FCT_RA_CUST_CITIZNSHPS

9. FCT_RA_MARKETS_SERVED

10. FCT_RA_PRODUCTS_OFFERED

11. FCT_RA_CUST_PHONES

12. FCT_RA_CUST_SRC_WEALTH_DTLS

13. FCT_RA_DOC_VERF_DTLS

14. FCT_RA_ACTIONS

15. FCT_TP_IDV_REQUESTS

16. FCT_TP_WLS_REQUESTS

17. FCT_TP_WLS_RESULTS

18. FCT_TP_NNS_REQUESTS

19. FCT_TP_NNS_RESULTS

20. FCT_RA_RISK_RATING_SUMMARY

21. FCT_TP_RISK_RATING_DETAILS

22. FCT_RA_RISK_RATING_REASONS

23. FCT_RA

CHAPTER 3 *Views*

Know Your Customer uses many Oracle database view definitions to process risk assessments. The following table provides a high-level description of the views:

Table 6. Views

View	Description
VW_DOCS_VERF_CUST_LIST	This view identifies the list of customers who are eligible for Mandatory Document Verification.
VW_IDV_REQUESTS	This view provides the consolidated list of customers for whom third- party ID verification should be initiated.
USRGPMAP	This view is used to show the mapping data of user and user group.
CSSMS_HOLIDAY_LIST	This view fetches the Holidays which the bank administrator has entered.
FCT_CUST_ACCT_DOCS	This view is created on the CUST_ID_DOC table of the Business schema. The view will display the type of documents each customer has provided during the account opening process.
VW_BUS_LATEST_ACCT	This view gets the date of the latest account of a customer.

Functions, Stored Procedures and Packages

Know Your Customer uses many Oracle functions and stored procedure definitions to process the risk assessment request received.

The following table describes these functions and procedures.

Table 7. Functions/Stored Procedures and Packages

Function/Stored Procedure/Package	Description
Fn_Working_Days	This function ensures that the selected next Re-Review date is a working date. If the calculated Re-Review date is a holiday, the customer will not be eligible for Periodic Re-Review processing. The next Re-Review date must be computed at the time of Auto-Closure.
FN_REREVIEW_DATE	This function is used to identify the periodic review date for Deployment Initiation customers by splitting the customer base into equal slices per day starting from the number of days defined in the attribute
FN_REGISTRATION_CHECK_DRR	This function checks for all the risk assessments where the difference between the processing date and the date when the risk assessed customer's records were last updated. If this date is greater than the threshold value specified in the Registration Task Minimum Period application parameter (KYC_CASE_REG_TASK_MIN_PRD), then the Registration Information Update Required Flag is set to Y and the RA status is set to HOLD.
FN_RB_PROCESSING	This function ensures that all the risk assessments eligible for Rule Base Processing are processed through the Rule based processing engine.
FN_RA_TO_CASE	This function will promote all the risk assessments from the KYC system when the CER score is beyond the limit defined to cases in the ECM system.
fn_ra_purge	This function will delete the data used for arriving at the risk score of all the closed risk assessments from various tables based on the parameters provided.
FN_PRCNG_TMP_WITH_IP_DR	This function will identify the Interested parties of the customers identified for risk assessment during the Regular processing batch.
FN_PRCNG_TMP_WITH_IP_DI	This function will identify the Interested parties of the customers identified for risk assessment during the Deployment initiation processing batch.
FN_PRCNG_ACT_DATA_LOAD	This function will load the data from the RA processing tables to the actual RA tables after the risk assessment process is complete.
FN_PARTITION_MAINTENANCE	This function will create and maintain the partition created on the FCT_CUST_RA_HISTRY table.
FN_LOG_MSG	This function is used to load the messages into the APPLN_LOG_MSGS table during the execution of the functions / procedures / packages.
FN_INCPRCDATEBYONE	This function will increment the KYC processing date by one day and keep the system ready for the next batch.

Table 7. Functions/Stored Procedures and Packages

Function/Stored Procedure/Package	Description
fn_get_case_owner	This function is used to identify the owner to whom the case must assigned during the Promote to case activity.
FN_DEL_DATA_FRM_PRCNG	This function will delete the data from the KYC processing table before the actual KYC batch processing is carried out.
FN_CUST_RA_HISTORY	This function will load the data of all the risk assessments created on all the customers on that particular day into the FCT_CUST_RA_HISTRY table.
FN_CLOSUREUPD_RALASTDATE	This function will update the last risk assessment date for all the risk assessments during the algorithm based risk assessment process.
FN_CLOSUREUPD_RACERSCORE	This function will update the CER score for all the risk assessments during the algorithm based risk assessment process.
FN_CLOSUREUPD_RACERPRIORITY	This function will update the priority for all the risk assessments during the algorithm based risk assessment process based on the CER score of the risk assessment.
FN_CLOSUREUPD_RACERCTGRYSCORE	This function will update the risk category based on the CER score for all the risk assessments during the algorithm based risk assessment process.
FN_CLOSURE_UPDATES	This function does the Closure Updation for the risk assessments for all the workflows.
FN_CCRCALC_UPDWTRSKSCORE	This function will update the Dynamic weighted risk score for all the risk assessments during the algorithm based risk assessment process.
FN_CCRCALC_UPDRSKSCORE	This function will update the Dynamic risk score for all the risk assessments during the algorithm based risk assessment process.
FN_CCRCALC_UPDDYNWT	This function will update the Dynamic weight for all the risk assessments during the algorithm based risk assessment process.
RISKRATINGROAR	This package is used for Real Time On-boarding Risk Assessment.

KYC Batches

This chapter covers the KYC Batch and the tasks within the batches. This chapter discusses the following topics:

- Regular Processing
- Deployment-Initiation-Processing
- End of Day Processing

Regular Processing

Table 8: Regular Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task1	FN_DEL_DATA_FRM_PRCNG	TRANS-FORM DATA	Truncate the data from KYC processing tables	Task1
Task2	RvwSuspCust_RR	LOAD DATA	Reasons based on alerts generated in Oracle Financial Services Behavior Detection Framework	Task2
Task3	RvwSuspAcct_RR	LOAD DATA	Reasons based on alerts generated in Oracle Financial Services Behavior Detection Framework	Task3
Task4	RvwFreqCust_RR	LOAD DATA	Reasons based on alerts generated in Oracle Financial Services Behavior Detection Framework	Task4
Task5	RvwFreqAcct_RR	LOAD DATA	Reasons based on alerts generated in Oracle Financial Services Behavior Detection Framework	Task5
Task6	RvwCustSAR_RR	LOAD DATA	Reasons based on alerts generated in Oracle Financial Services Behavior Detection Framework	Task6
Task7	RvwHighScoreCust_RR	LOAD DATA	Reasons based on alerts generated in Oracle Financial Services Behavior Detection Framework	Task7
Task8	RvwHighScoreAcct_RR	LOAD DATA	Reasons based on alerts generated in Oracle Financial Services Behavior Detection Framework	Task8
Task9	RvwCustStateChg_RR	LOAD DATA	Reasons based on change log summary in Oracle Financial Services Behavior Detection Framework	Task9
Task10	RvwAcctStateChg_RR	LOAD DATA	Reasons based on change log summary in Oracle Financial Services Behavior Detection Framework	Task10

Table 8: Regular Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task11	RvwCustCntyChg_RR	LOAD DATA	Reasons based on change log summary in Oracle Financial Services Behavior Detection Framework	Task11
Task12	RvwAcctCntyChg_RR	LOAD DATA	Reasons based on change log summary in Oracle Financial Services Behavior Detection Framework	Task12
Task13	RvwCustCtzChg_RR	LOAD DATA	Reasons based on change log summary in Oracle Financial Services Behavior Detection Framework	Task13
Task14	RvwIncCustAuth_RR	LOAD DATA	Reasons based on change log summary in Oracle Financial Services Behavior Detection Framework	Task10, Task11, Task12, Task13, Task14, Task2, Task3, Task4, Task5, Task6, Task7, Task8, Task9
Task15	CustIdentificationAcctOpn	LOAD DATA	Identify the customers for Risk assessment creation for New Accounts	Task15
Task16	CustIdentificationAccRvw	LOAD DATA	Identify the customers for Risk assessment creation for Accelerated re-review customers	Task16
Task17	CustIdentificationPrdRvw	LOAD DATA	Identify the customers for Risk assessment creation for Periodic re-review customers	Task17
Task18	HoldRAIdentification	LOAD DATA	Identify the Risk assessments which were cleared from HOLD status for Risk assessment process	Task15, Task16, Task17, Task18
Task19	FN_CUST_IP_PRCNG_DR	TRANSFORM DATA	Identify the interested parties for the risk assessed customers	Task19
Task20	CreateRA	LOAD DATA	Creation of the Risk assessments	Task20
Task21	RACreationAction	LOAD DATA	Log action for Risk assessment creation	Task21
Task22	InitAcctRvwDtls	LOAD DATA	Account Repository maintenance	Task22
Task23	InitCustRvwDtls	LOAD DATA	Customer Repository maintenance	Task20, Task21, Task22, Task23
Task24	CreateSnpCust	LOAD DATA	Copy snapshot of risk assessed customer	Task24
Task25	FN_Regestration_Check	TRANSFORM DATA	Identify if the risk assessed customer data is latest or old for the risk assessment process	Task25
Task26	AccountOpenDoc	TRANSFORM DATA	Documents required for Account Opening	Task26
Task27	CreateWlsReq	LOAD DATA	Create request for watch list processing for all the risk assessments	Task27

Table 8: Regular Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task28	Watchlist_FuzzyMatch	TRANS-FORM DATA	Invoking the AML fuzzy match utility to scan the customers who are extracted above	Task28
Task29	CreateWlsResult	LOAD DATA	Populate the results for the watch requests created	Task29
Task30	LogWlsAction	LOAD DATA	Log action for Watchlist scanning	Task30
Task31	CreateNnsReq	LOAD DATA	Create request for Negative News Search processing for all the risk assessments	Task31
Task32	NNS_Invoke	TRANS-FORM DATA	Invoke the external third party service for all the requests created and load the data in the results table	Task32
Task33	LogNnsAction	LOAD DATA	Log action for Negative News Search scanning	Task33
Task34	CpySnpAdr	LOAD DATA	Copy snapshot of the customer address for the risk assessed customer	Task34
Task35	CpySnpCustPhnMnts	LOAD DATA	Copy snapshot of the customer phone for the risk assessed customer	Task35
Task36	DocumentVerification	LOAD DATA	Identify verification is done for all the risk assessed customers based on the type of documents provided by the customer	Task36
Task37	DocumentVerificationAction	LOAD DATA	Log action for Document Verification scanning	Task37
Task38	CreateIdvReq	LOAD DATA	Create request for Identity verification processing for all the risk assessments	Task38
Task39	IDV_Invoke	TRANS-FORM DATA	Invoke the external third party service for all the requests created and load the data in the results table	Task39
Task40	LogIdvAction	LOAD DATA	Log action for Identity verification scanning	Task40
Task41	CpySnpCustCtz	LOAD DATA	Copy snapshot of the customer citizenship for the risk assessed customer	Task41
Task42	CpySnpAcctMnts	LOAD DATA	Copy snapshot of the customer accounts for the risk assessed customer	Task42
Task43	CpySnpCustSrcWlth	LOAD DATA	Copy snapshot of the customer source of wealth for the risk assessed customer	Task43
Task44	CpySnpAcctRoleMnts	LOAD DATA	Copy snapshot of the Role of customer on account for the risk assessed customer	Task44

Table 8: Regular Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task45	CpySnpCustRelMnts	LOAD DATA	Copy snapshot of the customer to customer relationship for the risk assessed customer	Task45
Task46	CpySnpCustCntyMnts	LOAD DATA	Copy snapshot of the customer country for the risk assessed customer	Task46
Task47	CpySnpCustMkt	LOAD DATA	Copy snapshot of the market served by the customer for the risk assessed customer	Task47
Task48	CpySnpCustPrd	LOAD DATA	Copy snapshot of the products provided by the customer for the risk assessed customer	Task48
Task49	LogSnapshotAction	LOAD DATA	Log action for snap shot	Task49
Task50	FN_RB_PROCESSING	TRANS-FORM DATA	Rule based risk assessment process	Task50
Task51	CCRCalc_CIP_Dtls	LOAD DATA	Algorithm based risk assessment process	Task51
Task52	CCRCalc_CIP_PC	LOAD DATA	Algorithm based risk assessment process	Task52
Task53	CCRCalc_CIP_IP	LOAD DATA	Algorithm based risk assessment process	Task53
Task54	CCRCalc_WLS_Dtls	LOAD DATA	Algorithm based risk assessment process	Task54
Task55	CCRCalc_WLS_PC	LOAD DATA	Algorithm based risk assessment process	Task55
Task56	CCRCalc_WLS_IP	LOAD DATA	Algorithm based risk assessment process	Task56
Task57	CCRCalc_NNS_Dtls	LOAD DATA	Algorithm based risk assessment process	Task57
Task58	CCRCalc_NNS_PC	LOAD DATA	Algorithm based risk assessment process	Task58
Task59	CCRCalc_NNS_IP	LOAD DATA	Algorithm based risk assessment process	Task59
Task60	CCRCalc_RelshpRsns	LOAD DATA	Algorithm based risk assessment process	Task60
Task61	CCRCalc_CorpAgeRsns	LOAD DATA	Algorithm based risk assessment process	Task61
Task62	CCRCalc_CntyOprRsns	LOAD DATA	Algorithm based risk assessment process	Task62
Task63	CCRCalc_CtzRsns	LOAD DATA	Algorithm based risk assessment process	Task63
Task64	CCRCalc_CntyHqRsns	LOAD DATA	Algorithm based risk assessment process	Task64
Task65	CCRCalc_CntyResRsns	LOAD DATA	Algorithm based risk assessment process	Task65
Task66	CCRCalc_CntyTaxRsns	LOAD DATA	Algorithm based risk assessment process	Task66

Table 8: Regular Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task67	CCRCalc_IndustryRsns	LOAD DATA	Algorithm based risk assessment process	Task67
Task68	CCRCalc_OccupationRsns	LOAD DATA	Algorithm based risk assessment process	Task68
Task69	CCRCalc_PubCompRsns	LOAD DATA	Algorithm based risk assessment process	Task69
Task70	CCRCalc_SrcWlthRsns	LOAD DATA	Algorithm based risk assessment process	Task70
Task71	CCRCalc_LegStrcRsns	LOAD DATA	Algorithm based risk assessment process	Task71
Task72	CCRCalc_MrktRsns	LOAD DATA	Algorithm based risk assessment process	Task72
Task73	CCRCalc_ProdRsns	LOAD DATA	Algorithm based risk assessment process	Task73
Task74	CCRCalc_CustCCRSmry	LOAD DATA	Algorithm based risk assessment process	Task74
Task75	FN_CCRCALC_UPDDYNWT	TRANSFORM DATA	Algorithm based risk assessment process	Task75
Task76	FN_CCRCALC_UPDRSKSCORE	TRANSFORM DATA	Algorithm based risk assessment process	Task76
Task77	FN_CCRCALC_UPDWTRSKSCORE	TRANSFORM DATA	Algorithm based risk assessment process	Task77
Task78	FN_CLOSUREUPD_RACERSCORE	TRANSFORM DATA	Algorithm based risk assessment process	Task78
Task79	FN_CLOSUREUPD_RACERCTGRY	TRANSFORM DATA	Algorithm based risk assessment process	Task79
Task80	FN_CLOSUREUPD_RACERPRIOR	TRANSFORM DATA	Algorithm based risk assessment process	Task80
Task81	FN_CLOSUREUPD_RALASTDATE	TRANSFORM DATA	Algorithm based risk assessment process	Task81
Task82	FN_CLOSURE_UPDATES	TRANSFORM DATA	Closure updated for the risk assessments created	Task82
Task83	LogModelBasedAction	LOAD DATA	Log action for Algorithm based risk assessment process	Task83
Task84	FN_RA_TO_CASE	TRANSFORM DATA	Promotion of the Risk assessment to a Case	Task84
Task85	Auto_Case_Assignment	TRANSFORM DATA	Invoking the Auto Case Assignment process of AML for assigning the cases to the users	Task85
Task86	FN_POST_CASE_ASSIGNMENT	TRANSFORM DATA	Updating the details of the cases after the case assignment process is complete	Task86

Table 8: Regular Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task87	FN_CUST_RA_HISTORY	TRANS-FORM DATA	Population of the data related to the Risk assessments created for the customer into the History table	Task87
Task88	FN_PRCNG_ACT_DATA_LOAD	TRANS-FORM DATA	Movement of the data from the Processing table to the Actual tables after the Risk assessment process	Task24, Task25, Task26, Task27, Task28, Task29, Task30, Task31, Task32, Task33, Task34, Task35, Task36, Task37, Task38, Task39, Task40, Task41, Task42, Task43, Task44, Task45, Task46, Task47, Task48, Task49, Task50, Task51, Task52, Task53, Task54, Task55, Task56, Task57, Task58, Task59, Task60, Task61, Task62, Task63, Task64, Task65, Task66, Task67, Task68, Task69, Task70, Task71, Task72, Task73, Task74, Task75, Task76, Task77, Task78, Task79, Task80, Task81, Task82, Task83, Task84, Task85, Task86, Task87, Task88
Task89	GenCustDetails_ED	EXTRACT DATA	Extract the Customer feedback details	Task89
Task90	GenWLSFeedback_ED	EXTRACT DATA	Extract the Watchlist scanning feedback details	Task90
Task91	GenCBSFeedback_ED	EXTRACT DATA	Extract customer details for CBS	Task91
Task92	FN_INCPRCDATEBYONE	TRANS-FORM DATA	Incrementing the KYC processing date by 1 day	Task92
Task93	KYC_File_Rename	TRANS-FORM DATA	Renaming of the extracted files according to the AML needs	Task93
Task94	FN_RA_PURGE	TRANS-FORM DATA	Purging of the Autoclosed or UI closed risk assessments	Task94
Task95	FN_PARTITION_MAINTENANCE	TRANS-FORM DATA	Dropping the partition on the FCT_CUST_RA_HISTRY table	N

Deployment-Initiation-Processing

Table 9: Deployment-Initiation-Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task1	FN_DEL_DATA_FRM_PRCNG	Truncate the data from KYC processing tables	TRANSFORM DATA	
Task2	CustIdentificationDI	Identify the customers for Risk assessment creation for DI	LOAD DATA	Task1
Task3	FN_CUST_IP_PRCNG_DI	Identify the interested parties for the risk assessed customers	TRANSFORM DATA	Task2
Task4	CreateRA	Creation of the risk assessments	LOAD DATA	Task3
Task5	RACreationAction	Log action for risk assessment creation	LOAD DATA	Task4
Task6	InitAcctRvwDtls	Account Repository maintenance	LOAD DATA	Task5
Task7	InitCustRvwDtls	Customer Repository maintenance	LOAD DATA	Task6
Task8	CreateSnpCust	Copy snapshot of risk assessed customer	LOAD DATA	Task4, Task5, Task6, Task7
Task9	AccountOpenDoc	Documents required for Account Opening	TRANSFORM DATA	Task8
Task10	CreateWlsReq	Create request for watch list processing for all the risk assessments	LOAD DATA	Task9
Task11	Watchlist_FuzzyMatch	Invoking the Oracle Financial Services Behavior Detection Framework fuzzy match utility to scan the customers who are extracted above	TRANSFORM DATA	Task10
Task12	CreateWlsResult	Populate the results for the watch requests created	LOAD DATA	Task11
Task13	LogWlsAction	Log action for Watchlist scanning	LOAD DATA	Task12
Task14	CpySnpAdr	Copy snapshot of the customer address for the risk assessed customer	LOAD DATA	Task13
Task15	CpySnpCustPhnMnts	Copy snapshot of the customer phone for the risk assessed customer	LOAD DATA	Task14
Task16	CpySnpCustCtz	Copy snapshot of the customer citizenship for the risk assessed customer	LOAD DATA	Task15
Task17	CpySnpAcctMnts	Copy snapshot of the customer accounts for the risk assessed customer	LOAD DATA	Task16
Task18	CpySnpCustSrcWlth	Copy snapshot of the customer source of wealth for the risk assessed customer	LOAD DATA	Task17
Task19	CpySnpAcctRoleMnts	Copy snapshot of the Role of customer on account for the risk assessed customer	LOAD DATA	Task18

Table 9: Deployment-Initiation-Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task20	CpySnpCustRelMnts	Copy snapshot of the customer to customer relationship for the risk assessed customer	LOAD DATA	Task19
Task21	CpySnpCustCntyMnts	Copy snapshot of the customer country for the risk assessed customer	LOAD DATA	Task20
Task22	CpySnpCustMkt	Copy snapshot of the market served by the customer for the risk assessed customer	LOAD DATA	Task21
Task23	CpySnpCustPrd	Copy snapshot of the products provided by the customer for the risk assessed customer	LOAD DATA	Task22
Task24	LogSnapshotAction	Log action for snap shot	LOAD DATA	Task23
Task25	FN_RB_PROCESSING	Rule based risk assessment process	TRANSFORM DATA	Task24
Task26	CCRCalc_CIP_Dtls	Algorithm based risk assessment process	LOAD DATA	Task25
Task27	CCRCalc_CIP_PC	Algorithm based risk assessment process	LOAD DATA	Task26
Task28	CCRCalc_CIP_IP	Algorithm based risk assessment process	LOAD DATA	Task27
Task29	CCRCalc_WLS_Dtls	Algorithm based risk assessment process	LOAD DATA	Task28
Task30	CCRCalc_WLS_PC	Algorithm based risk assessment process	LOAD DATA	Task29
Task31	CCRCalc_WLS_IP	Algorithm based risk assessment process	LOAD DATA	Task30
Task32	CCRCalc_RelshpRsns	Algorithm based risk assessment process	LOAD DATA	Task31
Task33	CCRCalc_CorpAgeRsns	Algorithm based risk assessment process	LOAD DATA	Task32
Task34	CCRCalc_CntyOprRsns	Algorithm based risk assessment process	LOAD DATA	Task33
Task35	CCRCalc_CtzRsns	Algorithm based risk assessment process	LOAD DATA	Task34
Task36	CCRCalc_CntyHqRsns	Algorithm based risk assessment process	LOAD DATA	Task35
Task37	CCRCalc_CntyResRsns	Algorithm based risk assessment process	LOAD DATA	Task36
Task38	CCRCalc_CntyTaxRsns	Algorithm based risk assessment process	LOAD DATA	Task37
Task39	CCRCalc_IndustryRsns	Algorithm based risk assessment process	LOAD DATA	Task38
Task40	CCRCalc_OccupationRsns	Algorithm based risk assessment process	LOAD DATA	Task39
Task41	CCRCalc_PubCompRsns	Algorithm based risk assessment process	LOAD DATA	Task40

Table 9: Deployment-Initiation-Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task42	CCRCalc_SrcWlthRsns	Algorithm based risk assessment process	LOAD DATA	Task41
Task43	CCRCalc_LegStrcRsns	Algorithm based risk assessment process	LOAD DATA	Task42
Task44	CCRCalc_MrktRsns	Algorithm based risk assessment process	LOAD DATA	Task43
Task45	CCRCalc_ProdRsns	Algorithm based risk assessment process	LOAD DATA	Task44
Task46	CCRCalc_CustCCRSmry	Algorithm based risk assessment process	LOAD DATA	Task45
Task47	FN_CCRCALC_UPDDYNWT	Algorithm based risk assessment process	TRANSFORM DATA	Task46
Task48	FN_CCRCALC_UPDRSKSCORE	Algorithm based risk assessment process	TRANSFORM DATA	Task47
Task49	FN_CCRCALC_UPDWTRSKSCORE	Algorithm based risk assessment process	TRANSFORM DATA	Task48
Task50	FN_CLOSUREUPD_RACERSCORE	Algorithm based risk assessment process	TRANSFORM DATA	Task49
Task51	FN_CLOSUREUPD_RACERCTGRY	Algorithm based risk assessment process	TRANSFORM DATA	Task50
Task52	FN_CLOSUREUPD_RACERPRIOR	Algorithm based risk assessment process	TRANSFORM DATA	Task51
Task53	FN_CLOSUREUPD_RALASTDATE	Algorithm based risk assessment process	TRANSFORM DATA	Task52
Task54	FN_CLOSURE_UPDATES	Closure updated for the risk assessments crated	TRANSFORM DATA	Task53
Task55	LogModelBasedAction	Log action for Algorithm based risk assessment process	LOAD DATA	Task54
Task56	FN_RA_TO_CASE	Promotion of the Risk assessment to a Case	TRANSFORM DATA	Task55
Task57	Auto_Case_Assignment	Invoking the Auto Case Assignment process of Oracle Financial Services Behavior Detection Framework for assigning the cases to the users	TRANSFORM DATA	Task56
Task58	FN_POST_CASE_ASSIGNMENT	Updating the details of the cases after the case assignment process is complete	TRANSFORM DATA	Task57
Task59	FN_CUST_RA_HISTORY	Population of the data related to the Risk assessments created for the customer into the History table	TRANSFORM DATA	Task58
Task60	FN_PRCNG_ACT_DATA_LOAD	Movement of the data from the Processing table to the Actual tables after the Risk assessment process	TRANSFORM DATA	Task59

End of Day Processing

Table 10: End of Day Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task1	GenCustDetails_ED	Extract the customer feedback details	EXTRACT DATA	
Task2	GenWLSFeedback_ED	Extract the Watchlist scanning feedback details	EXTRACT DATA	Task1
Task3	GenCBSFeedback_ED	Extract customer details for CBS	EXTRACT DATA	Task2
Task4	FN_INCPRCDATEBYONE	Incrementing the KYC processing date by 1 day	TRANSFORM DATA	Task3
Task5	KYC_File_Rename	Renaming of the extracted files according to the AML needs	TRANSFORM DATA	Task4
Task6	FN_RA_PURGE	Purging of the Autoclosed or UI closed risk assessments	TRANSFORM DATA	Task5
Task7	FN_PARTITION_MAINTENANCE	Droping the partition on the FCT_CUST_RA_HISTRY table	TRANSFORM DATA	Task6
Task8	FN_REREVIEW_DATE_DI	Spliting of the customers processed through the DI processing back for periodic re-review	TRANSFORM DATA	Task7

Excel Upload Templates

This chapter discusses the following topics:

- Excel Upload Templates

Excel Upload Templates

The Excel Upload activity must be done in a specific order for certain templates. The order of the excel upload is as below:.

Table 11: List of Excel Upload Templates

Table Name	Excel Upload Template	Excel Mapping Name
DIM_JURISDICTION	DIM_JURISDICTION.xls	DIM_JURISDICTION.xml
DIM_CUSTOMER_TYPE	DIM_CUST_TYP.xls	DIM_CUSTOMER_TYPE.xml
DIM_COUNTRY	DIM_COUNTRY.xls	DIM_COUNTRY_KYC.xml
APPLN_INSTALL_PARAMS	APPLN_INSTALL_PARAMS.xls	APPLN_INSTALL_PARAMS.xml
APPLN_PARAMS	APPLN_PARAMS.xls	APPLN_PARAMS.xml
APPLN_RB_PROCESSING	APPLN_RB_PROCESSING.xls	APPLN_RB_PROCESSING.xml
APPLN_REREVIEW_PARAMS	APPLN_REREVIEW_PARAMS.xls	APPLN_REREVIEW_PARAMS.xml
APPLN_RISK_RATING_PARAMS	APPLN_RISK_RATING_PARAMS.xls	APPLN_RISK_RATING_PARAMS.xml
DIM_ACCOUNT_TYPE	DIM_ACCOUNT_TYPE.xls	DIM_ACCOUNT_TYPE.xml
DIM_ACCT_CUST_ROLE_TYPE	DIM_ACCT_CUST_ROLE_TYPE.xls	DIM_ACCT_CUST_ROLE_TYPE.xml
DIM_ACTION	DIM_ACTION.xls	DIM_ACTION_KYC.xml
DIM_ADDRESS_TYPE	DIM_ADDRESS_TYPE.xls	DIM_ADDRESS_TYPE_KYC.xml
DIM_CITIZENSHIP_STATUS	DIM_CITIZENSHIP_STATUS.xls	DIM_CITIZENSHIP_STATUS.xml
DIM_COMPANY_TYPE_RISK	DIM_COMPANY_TYPE_RISK.xls	DIM_COMPANY_TYPE_RISK.xml
DIM_CORP_AGE_RANGE	DIM_CORP_AGE_RANGE.xls	DIM_CORP_AGE_RANGE.xml
DIM_CTZNSHP_STATUS_DOC_VERF	DIM_CTZNSHP_STATUS_DOC_VERF.xls	DIM_CTZNSHP_STATUS_DOC_VERF.xml
DIM_DOCUMENT_TYPE	DIM_DOCUMENT_TYPE.xls	DIM_DOCUMENT_TYPE_KYC.xml
DIM_INCOME_SRC_TYPES	DIM_INCOME_SRC_TYPES.xls	DIM_INCOME_SRC_TYPES.xml
DIM_INDUSTRY	DIM_INDUSTRY.xls	DIM_INDUSTRY_KYC.xml
DIM_LGLSTRUC_OWNRSHP_RISK	DIM_LGLSTRUC_OWNRSHP_RISK.xls	DIM_LGLSTRUC_OWNRSHP_RISK.xml
DIM_MARKETS_SERVED	DIM_MARKETS_SERVED.xls	DIM_MARKETS_SERVED.xml
DIM_NEG_NEWS_RANGE	DIM_NEG_NEWS_RANGE.xls	DIM_NEG_NEWS_RANGE.xml
DIM_OCCUPATION	DIM_OCCUPATION.xls	DIM_OCCUPATION_KYC.xml
DIM_PHONE_TYPE	DIM_PHONE_TYPE.xls	DIM_PHONE_TYPE.xml
DIM_PRODUCT	DIM_PRODUCT.xls	DIM_PRODUCT_KYC.xml
DIM_RAORRISK_CATEGORY	DIM_RAORRISK_CATEGORY.xls	DIM_RAORRISK_CATEGORY.xml
DIM_RA_PRIORITY	DIM_RA_PRIORITY.xls	DIM_RA_PRIORITY.xml

Table 11: List of Excel Upload Templates

Table Name	Excel Upload Template	Excel Mapping Name
DIM_RA_SOURCE	DIM_RA_SOURCE.xls	DIM_RA_SOURCE.xml
DIM_RELATIONSHIP_TYPE	DIM_RELATIONSHIP_TYPE.xls	DIM_RELATIONSHIP_TYPE.xml
DIM_RELN_PERIOD_RANGE	DIM_RELN_PERIOD_RANGE.xls	DIM_RELN_PERIOD_RANGE.xml
DIM_RISK_CATEGORY	DIM_RISK_CATEGORY.xls	DIM_RISK_CATEGORY.xml
DIM_STATUS	DIM_STATUS.xls	DIM_STATUS_KYC.xml
DIM_TAX_IDENT_FORMAT	DIM_TAX_IDENT_FORMAT.xls	DIM_TAX_IDENT_FORMAT.xml
DIM_WLS_FEEDBACK	DIM_WLS_FEEDBACK.xls	DIM_WLS_FEEDBACK.xml
MAP_COMPANY_TYPE_JRSDCN	MAP_COMPANY_TYPE_JRSDCN.xls	MAP_COMPANY_TYPE_JRSDCN.xml
MAP_CORP_AGE_RANGE_JRSDCN	MAP_CORP_AGE_RANGE_JRSDCN.xls	MAP_CORP_AGE_RANGE_JRSDCN.xml
MAP_COUNTRY_JRSDCN	MAP_COUNTRY_JRSDCN.xls	MAP_COUNTRY_JRSDCN.xml
MAP_INCOME_SRC_TYPES_JRSDCN	MAP_INCOME_SRC_TYPES_JRSDCN.xls	MAP_INCOME_SRC_TYPES_JRSDCN.xml
MAP_INDUSTRY_JRSDCN	MAP_INDUSTRY_JRSDCN.xls	MAP_INDUSTRY_JRSDCN.xml
MAP_LGLSTRUC_OWNRSHP_JRSDCN	MAP_LGLSTRUC_OWNRSHP_JRSDCN.xls	MAP_LGLSTRUC_OWNRSHP_JRSDCN.xml
MAP_MARKETS_SERVED_JRSDCN	MAP_MARKETS_SERVED_JRSDCN.xls	MAP_MARKETS_SERVED_JRSDCN.xml
MAP_NNS_RANGE_JRSDCN	MAP_NNS_RANGE_JRSDCN.xls	MAP_NNS_RANGE_JRSDCN.xml
MAP_OCCUPATION_JRSDCN	MAP_OCCUPATION_JRSDCN.xls	MAP_OCCUPATION_JRSDCN.xml
MAP_PRODUCT_JRSDCN	MAP_PRODUCT_JRSDCN.xls	MAP_PRODUCT_JRSDCN.xml
MAP_RELN_PERIOD_RANGE_JRSDCN	MAP_RELN_PERIOD_RANGE_JRSDCN.xls	MAP_RELN_PERIOD_RANGE_JRSDCN.xml
VW_APPLN_PARAMS	VW_APPLN_PARAMS.xls	VW_APPLN_PARAMS.xml
VW_APPLN_REREVIEW_PARAMS	VW_APPLN_REREVIEW_PARAMS.xls	VW_APPLN_REREVIEW_PARAMS.xml
VW_APPLN_RISK_RATING_PARAMS	VW_APPLN_RISK_RATING_PARAMS.xls	VW_APPLN_RISK_RATING_PARAMS.xml
FCT_DOCS_GUIDELINES	FCT_DOCS_GUIDELINES.xls	FCT_DOCS_GUIDELINES.xml

APPENDIX C   *Configurability*

This chapter discusses the following topics:

- Application Related Configuration

- OFSAAI Related Configuration

- Application Configuration using OFSAAI Configurability

Configurability of the OFS KYC can be categorized in the following ways:

- Application Related

- OFSAAI Related

Application Related Configuration

KYC risk assessments requires some inputs from application parameters and installation parameters which can be defined by the admin user from the user interface.

For more information, refer to the *Configuration Guide*.

OFSAAI Related Configuration

The OFSAAI allows you to perform the following tasks:

- Incremental model changes:

  - Add - No Impact

  - Modify - Data dependency dictated by the back-end DB and manual un-mapping and mapping of metadata.

  - Delete - Data dependency dictated by the back-end DB and manual un-mapping and mapping of metadata.

- ETL Changes:

  - Add

  - Change

  - Delete

- Definition of Excel Upload mapping to push data into the Database.

- Files and tables based on Source Data Definition.

- Metadata Data Maintenance:

  - Add

  - Modify

  - Delete

- Operations Administration:

    - Batch Scheduling flexibility

    - Hold or delete tasks from the batch.(For Example: Insert, Update Rules, Custom Executable, and Procedures)

    - Changes to User or User Group Function and Role definitions and mapping.

- UI and Workflow Maintenance

Note: Changes to UI and workflow definitions requires knowledge of OFSAAI specific editors in addition to the knowledge of OFS KYC and the OFSAAI.

The following figure displays mapping used to push data into the application Database periodically:
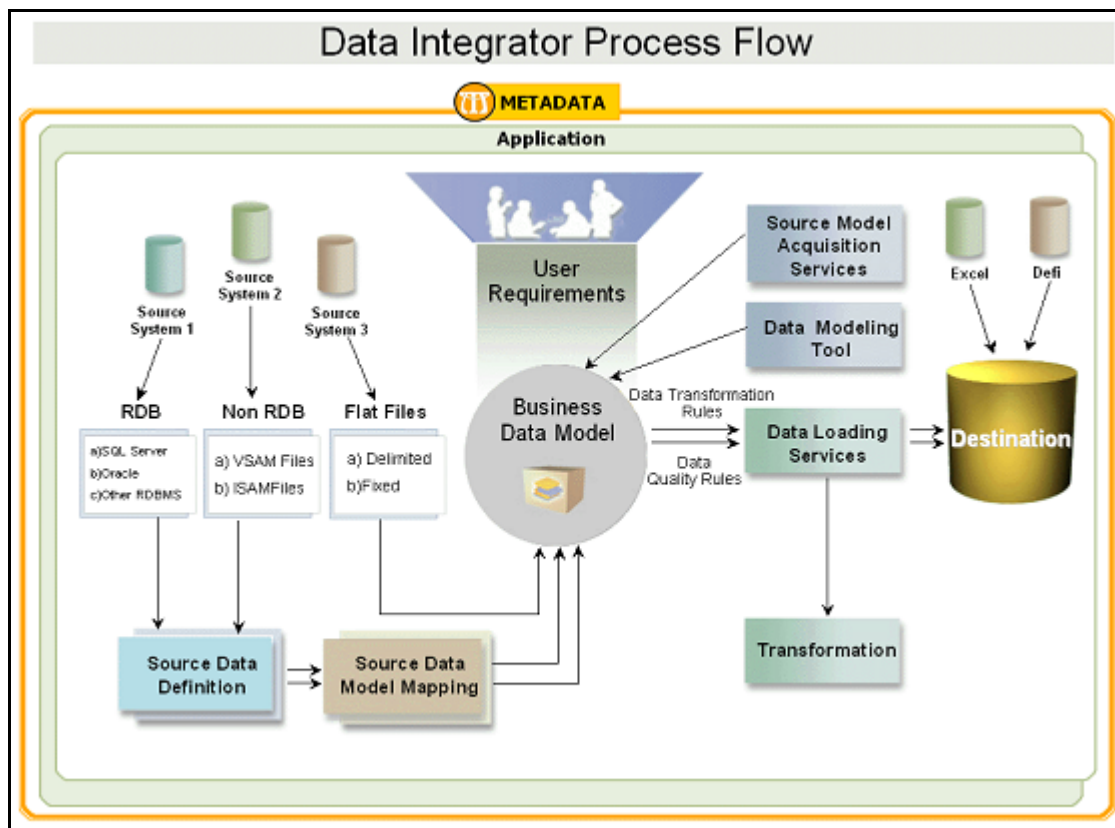
Figure 11. Data Integrator Process Flow

The following figure illustrates basic metadata, derived entity, rules, and reports:
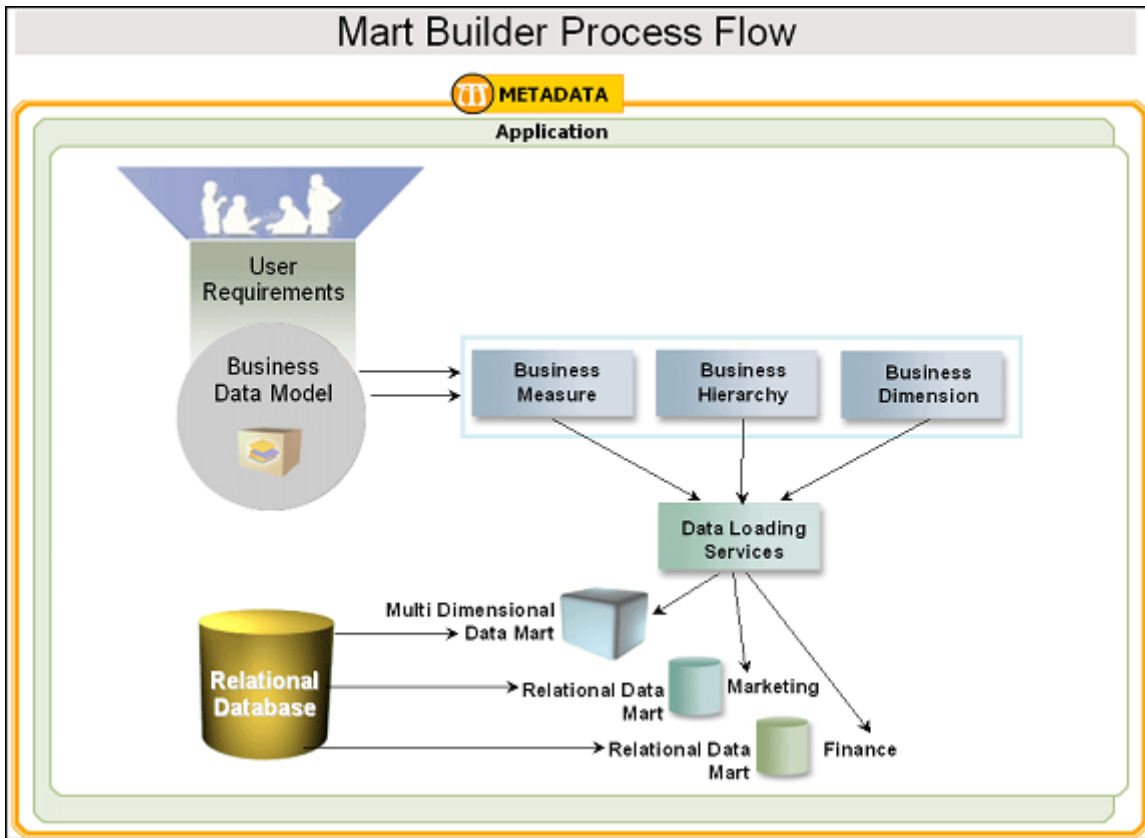
Figure 12. Mart Builder Process Flow
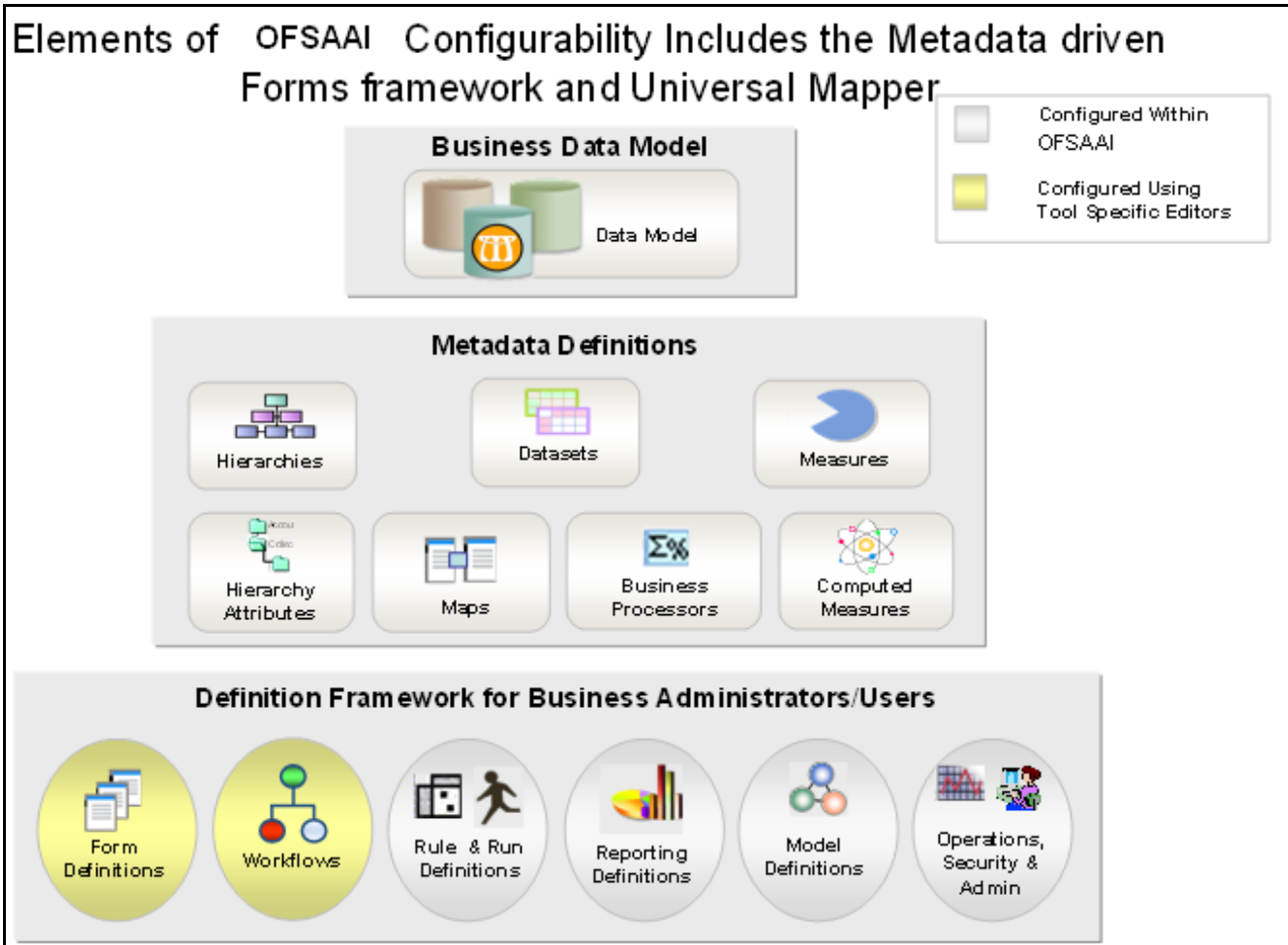
Figure 13. Elements of OFSAAI Configurability

Application Configuration using OFSAAI Configurability

- Web Service Call (Real Time Account On boarding Risk):
    - Data model changes, as applicable, to add an additional column or table
    - Revisions to Service Guide
    - Request and Response template corrections related to the Third Party service
    - Communication with the Source systems regarding the revisions of request and response formats
    - Testing of the revised request and response
- Additional Risk Models / Risk Parameters:
    - Data model changes as applicable, to add an additional columns or tables
    - Changes to File Based Data Ingestion / Web Service based Ingestion as explained above
    - Complete knowledge of how the System is designed (Data Model Knowledge)

Note: The Risk Assessment Module is configured using the OFSAAI Rules FW.

- Creation / Modification of Type 1 Rules:
    - Revision to Join as applicable
    - Filter correction, to remove or add an additional filter
    - Mapping of columns
- Creation/Modification of Type 2 and 3 Rules (Classification and Computational Rules):
    - Revision to Process Tree (to add/modify tasks and task sequence)
    - Revision to the run definition
    - Revision to the configurable values such model code / model parameter, Risk Weight
    - UI for maintaining the Risk modes and Risk Parameters
    - UI for maintaining the parameter Risk Values
    - Related Documentation revision
- Modification to the Pre-configured Risk Models - Slight Change in Logic:
    - Enhancing / changing the filter condition require all the steps mentioned above, except changes to the DM and related changes.
- Additions to Pre-Configured Re-Review Processing:
    - Additional derived entity definitions based on the Oracle Financial Services Alert Management System.
    - Complete knowledge of how the system is designed (Data Model Knowledge) for Re-Review processing.
    - Re-Review Processing is configured using the OFSAAI Rules FW.
- Creation/Modification of Type 1 Rules:
    - Revision to Join as applicable
    - Filter correction, to remove or add an additional filter
    - Mapping of columns

- Creation / Modification of Type 2 and 3 Rules (Classification and Computational Rules):

  - Revision to Process Tree (to add / modify tasks and task sequence)

  - Revision to the run definition

  - UI for maintaining the Re-Review Rules and parameters

  - Related Documentation revision

- Changes to Pre-Configured Re-Review Processing Models - Slight Change in Logic:

  - Enhancing or changing the filter condition requires all the steps mentioned above, except changes to the DM and related changes.

- Process Flow Changes:

  - All batch workflows (Default Review / Re-Review / Feedback Processing) are configured using the OFSAAI Rules FW

These steps must be executed depending on the type of change.

APPENDIX D   *Extraction Definition*

This chapter discusses the following topics:

- Extraction

Extraction

To set the delimiter used in the extraction files, follow these steps:

1. Log in as a KYC Administrator.

2. Navigate to the following path:

   ```
   Unified Metadata Manager> Technical Metadata Management> Data Integrator> Source
   Designer> Define Extracts.
   ```

3. Select and open the extraction from the list.

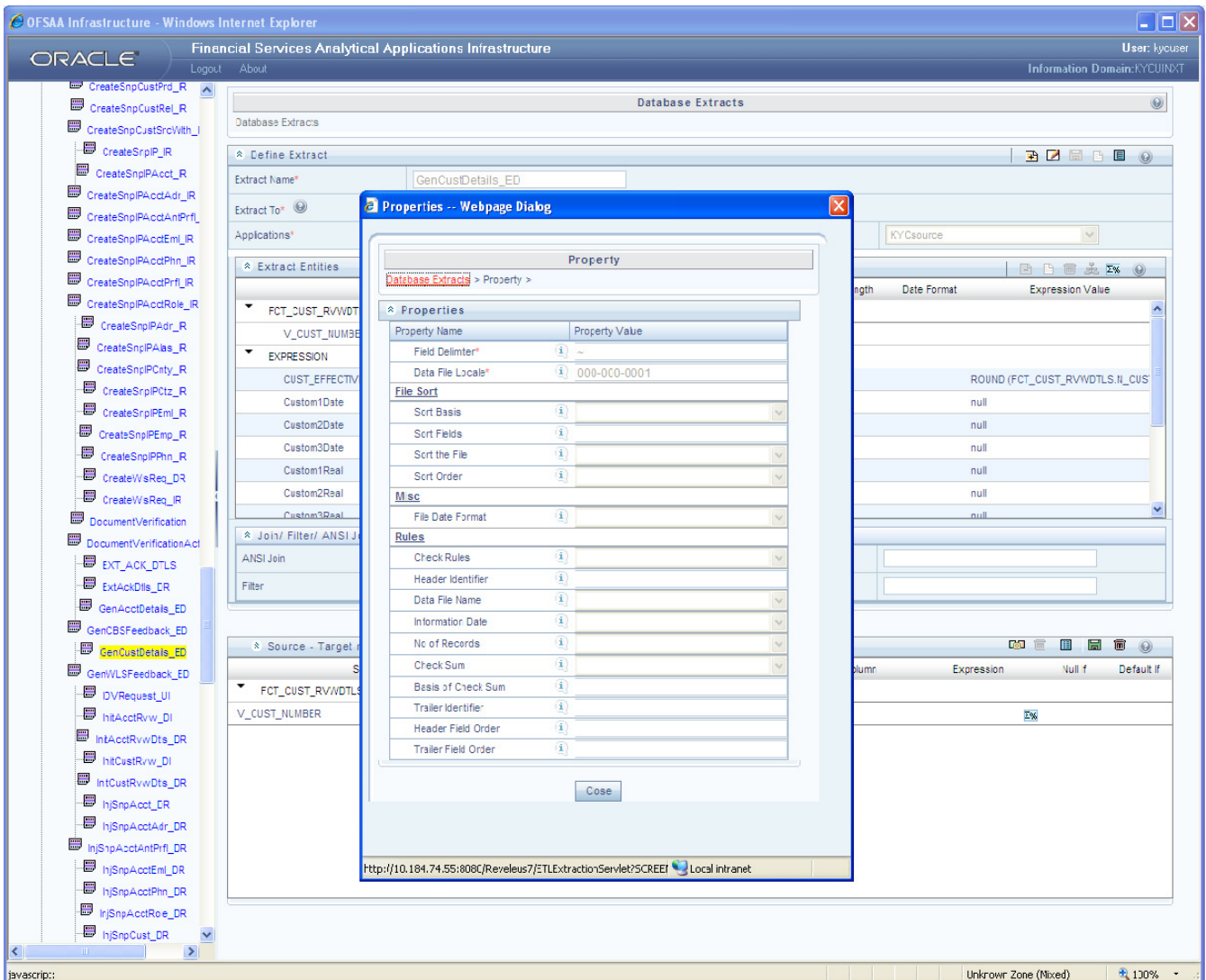**Figure 14. Extraction Definition**

Figure 15. Extract Properties

4. Click **Properties**. A pop-up window opens and lists the properties of the extraction.

5. Set the required delimiter and save the extraction.

Resaving Runs

The Oracle Financial Services KYC defines the following runs:

- Deployment-Initiation-Processing
- Regular-Processing
- EOD-Processing

The following section provide the steps to resave the run. The steps provided below are for resaving of Deployment-Initiation-Processing run. Follow the same steps to resave the Regular-Processing and EOD-Processing runs.

Resaving Runs

To resave runs, follow these steps:

1. Login to the OFS KYC as the KYC Admin user.
2. Navigate to **Rules Framework** and click **Designer**. The Rules Framework pop-up window appears.
3. In the pop-up window, click **Run**. The RUN screen displays in the RHS.
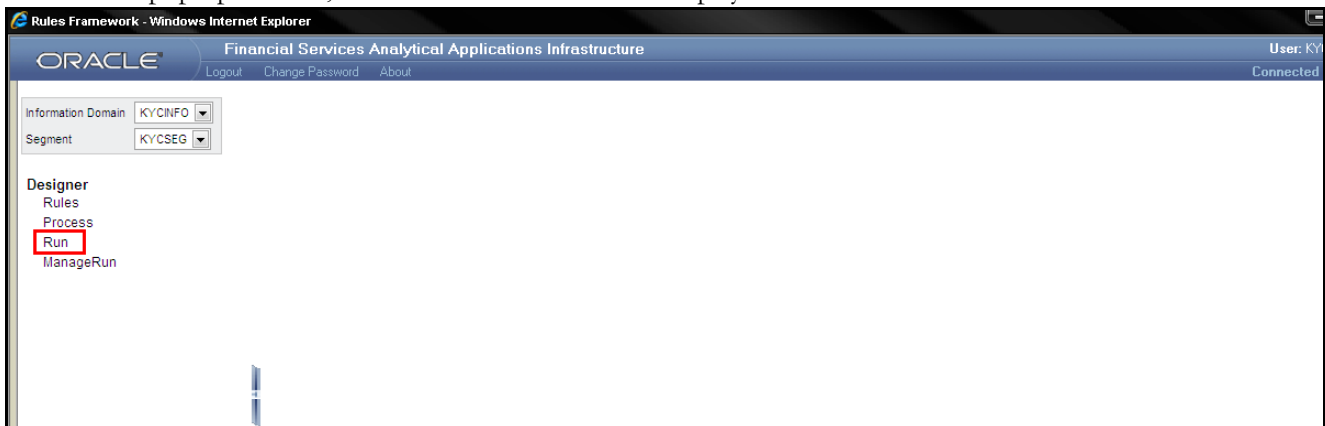

Figure 16. RUN screen

4. Click **Open**. The Open a Run pop-up window displays.
5. Select the Base Line Run radio button.
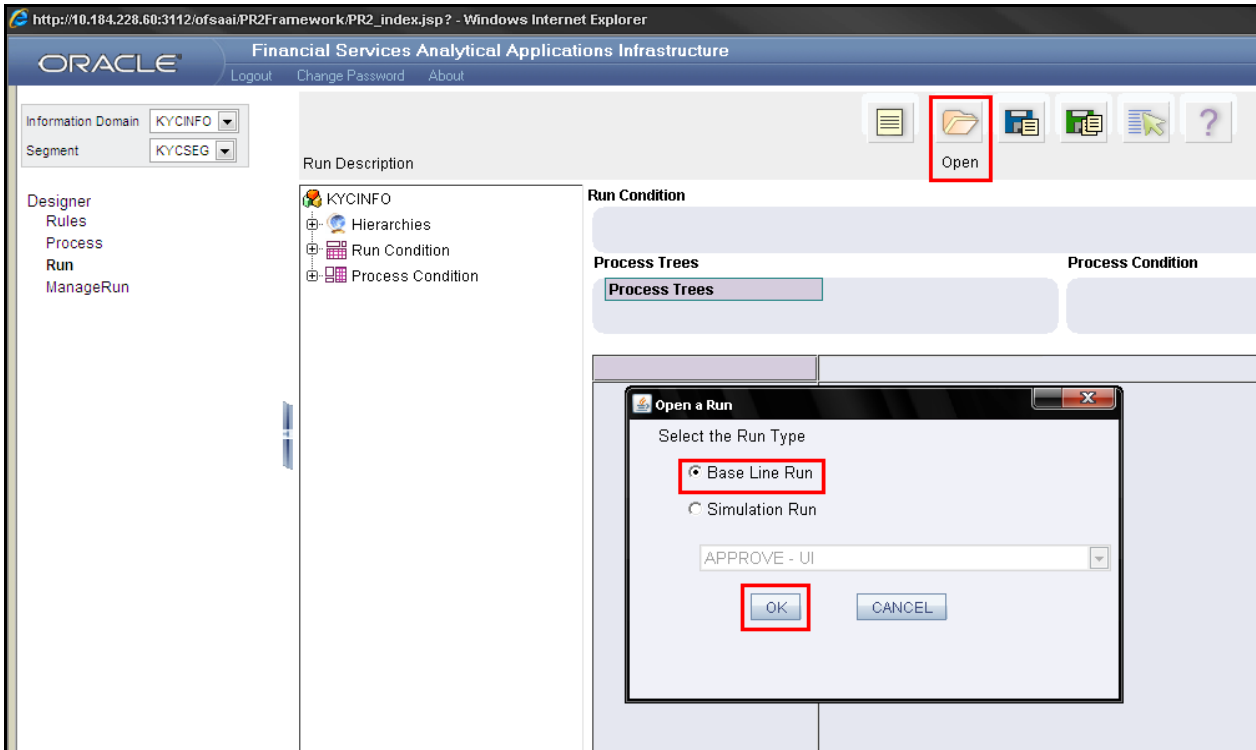6. Click **OK.** The Information Domains pop-up window displays.

Figure 17. Information Domains

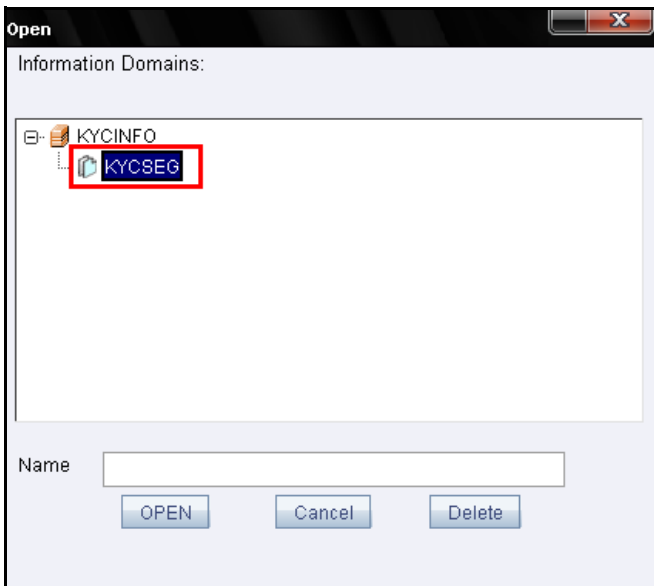7. Click the highlighted segment name.

Figure 18. File Name

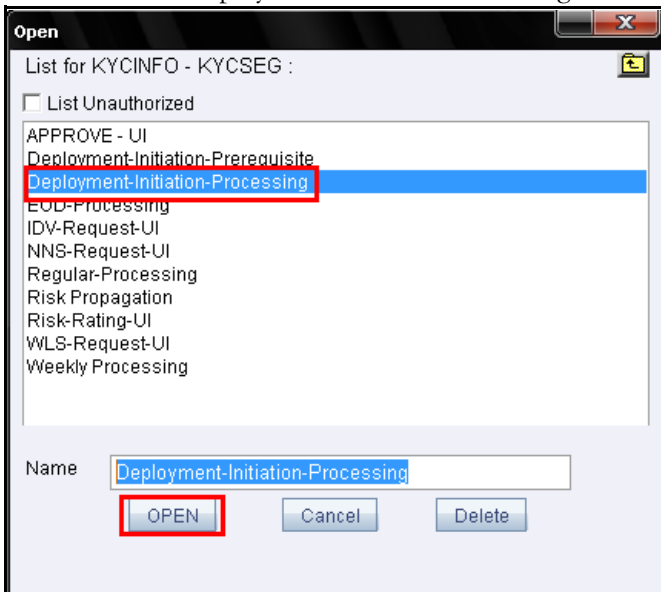8. Select the Deployment-Initiation-Processing Run.

Figure 19. Deployment-Initiation-Processing Run

9. Once the Run opens, click **Save**. A pop-up window displays.

10. Select the **Immediate batch Creation Mode** checkbox and the **Create batch with run-rule tasks** radio button, and click **Save**.

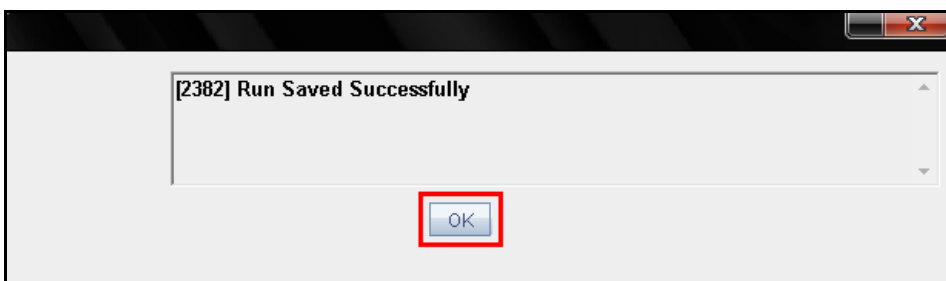11. Click **OK** to close the confirmation message.

Figure 20. Confirmation Message

12. Close the Rules Framework screen.

13. From the **Operations** menu, click **Batch Execution** and verify the resaved batches are visible in the Batch Execution screens.

If the batches are not visible, navigate to the Administration >Utilities> UserGroup-Batch Execution Map screen and execute the following steps:.

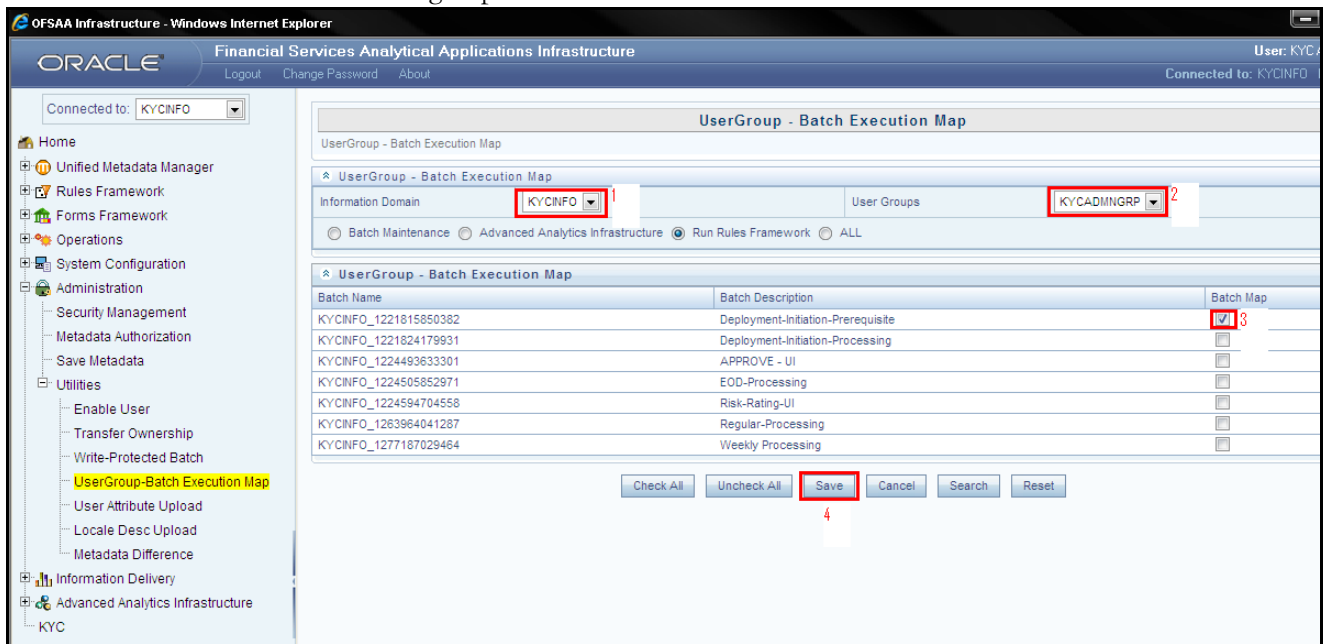**Figure 21. Batch Execution Map Screen**

    a. Select the KYC Infodom from the dropdown.

    b. Select the KYC Admin Group.

    c. Select the runs.

    d. Click **Save**.

      The resaved batches should be visible in the Batch Execution screen.

APPENDIX F   *KYC Batch Execution Logs*

This section provides the information on where log files are created for each type of task in the Oracle Financial Services KYC.

Logs are created only after the batches are executed. The following types of tasks are present in the batches:

- Table 2 Table (T2T)
- File 2 Table (F2T)
- Transform Data (DT)
    - SQL Function execution
    - Shell Script execution
- Table 2 File (T2F)
- Run Rule (PR2 Rule)

Batch Execution Logs are based on the types of rule. The following sections describe the types of task present in the batches:

Table 2 Table (T2T)

The logs for this type of task will be created in the path as follows:

`<Ofsaai Installed Area>/ficdb/log/ t2t/KYC12DOM_1221824179931_20121122_1_Task1_ttl.log`

The following table describes the log file:

Table 12: Table 2 Table (T2T)

Component	Description
KYC12DOM	This is the INFODOM on which the batch was executed
1221824179931	This is the ID of the RUN (batch is created once the RUN is saved)
20121122	This is the date on which the Batch was executed
1	The batch is executed for the first time on the same day
Task1	This log file is for the Task1 of the batch

File 2 Table (F2T)

The logs for this type of task will be created in the path as follows:

`<Ofsaai Installed Area>/ficdb/log/dmas/ DS_KYC12DOM_1263964041287_20121120_2_Task2.log`

Table 13: File 2 Table (F2T)

Component	Description
DS	This is a product indication for the type of log
KYC12DOM	This is the INFODOM on which the batch was executed
1263964041287	This is the ID of the RUN (batch is created once the RUN is saved)
20121120	This is the date on which the Batch was executed
2	The batch is executed for the second time on the same day
Task2	This log file is for the Task2 of the batch

In addition to this log, the following logs and files are created for the F2T type of tasks:

- `control=/ftpshare/KYC12DOM/scripts/load/ACCOUNT_OPEN/ExtAcct_DR.ctl` The data will be loaded into the table as per this control file, this file is provided by the Installer.

- `data=/ftpshare/STAGE/ACCOUNT_OPEN/20121121/ExtAcct_DR.dat` This is the file provide by the client.

- `bad=/ftpshare/STAGE/ACCOUNT_OPEN/20121121/ ExtAcct_DR.bad` This file will be created only if any of the data is rejected from the actual dat file.

- `log=/ftpshare/ACCOUNT_OPEN/20121121/F2T-TEST_dat.log` This log file provides the information on how many records are loaded and how many are rejected, also the reason why the data is not loaded.

Transform Data (Data transformation or DT logs)

The logs for this type of task will be created in the path as follows.

The following types of definitions can be defined under data transformations:

- Executing a Stored procedure
- Executing a Shell script

The following log files are created for the Stored Procedure execution type of Transform data. The definition name will be available in these log files.

- `<Ofsaai Installed Area>/ficdb/log/date/DT_KYC12DOM_1221824179931_20121123_1_Task23.log`
- `<Ofsaai Installed Area>/ficdb/log/date/RunProc_KYC12DOM_1221824179931_20121123_1_Task23.log`
- `/ftpshare/<DT_Definition_name>.log /`

Table 2 File (Extraction of Data)
Appendix A—KYC Batches

The following logs are created for the Shell script type of Transform data:

`<Ofsaai Installed Area>/ficdb/log/date/DT_KYC12DOM_1221824179931_20121123_1_Task23.log`

Information related to the failure will be inserted into the `am_log_file.logfile` which is present in the path `<Ofsaai Installed Area>/ficdb/log/`

Table 14: Shell script Transform data

Component	Description
DT	This is a product indication for the Data transformation type of log
RunProc	This indicated that the log is for running a procedure (function)
KYC12DOM	This is the INFODOM on which the batch was executed
1263964041287	This is the ID of the RUN (batch is created once the RUN is saved)
20121120	This is the date on which the Batch was executed
2	The batch is executed for the second time on the same day
Task23	This log file is for the Task23 of the batch
DT_Definition_name	A log file will be created with the name of the DT definition created.

Table 2 File (Extraction of Data)

The logs for this type of task will be created in the path as follows:

`<Ofsaai Installed Area>/ficdb/log/extraction/`
`KYC12DOM_1263964041287_20121122_2_Task24_ext.log`

Table 15: Table 2 File (Extraction of Data)

Component	Description
KYC12DOM	This is the INFODOM on which the batch was executed
1263964041287	This is the ID of the RUN (batch is created once the RUN is saved)
20121122	This is the date on which the Batch was executed
2	The batch is executed for the second time on the same day
Task24	This log file is for the Task24 of the batch
ext	This means that the log files is for extraction type of task

A log file with the name of the task executed will be generated in the following path:
`/ftpshare/STAGE/KYCsource/`

For Example:

`GenCBSFeedback_ED.log`

Run Rule (PR2 rule - Update Rule)

The logs for this type of task will be created in the path as follows.

`<Ofsaai Installed Area>/ficdb/log/runrule/KYC12DOM_1224493633301_20121115_1_Task1_PR2.LOG`

Table 16: Run Rule (PR2 rule - Update Rule)

Component	Description
KYC12DOM	This is the INFODOM on which the batch was executed
1224493633301	This is the ID of the RUN (batch is created once the RUN is saved)
20121115	This is the date on which the Batch was executed
1	The batch is executed for the first time on the same day
Task1	This log file is for the Task1 of the batch
PR2	This is a PR2 type of log. Log file for the definition created through PR2 framework

Promote to Case

If any of the risk assessments are not promoted to a case, refer to the table RA_TO_CASE_ERROR present in the KYC Atomic schema for the reasons for not being promoted.