

Oracle® Banking Party Management

Functional Overview

Release 2.7.0.0.0

F11757-01

March 2019

Oracle Banking Party Management Functional Overview, Release 2.7.0.0.0

F11757-01

Copyright © 2019 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	8
Audience	8
Documentation Accessibility	8
Related Documents	8
Conventions	8
1 Overview	11
2 Party Bank Policy (Fast Path: PI314)	13
3 Bank Policy	17
4 Party Maintenances	19
4.1 Relationship Maintenance (Fast Path: PI020)	19
4.2 Relationship Rules Definition (Fast Path: PI021)	19
4.3 Role Master (Fast Path: PI014)	20
4.4 Bureau Maintenance (Fast Path: PI099)	20
4.5 Manage Groups (Fast Path: PI024)	20
4.6 Financial Maintenance	21
4.6.1 Financial Category Maintenance (Fast Path: PI027)	21
4.6.2 Financial Nature Maintenance (Fast Path: PI790)	21
4.6.3 Financial Parameter Codes (Fast Path: PI791)	21
4.6.4 Financial Statement Template (Fast Path: PI794)	22
4.6.5 Financial Statement Template (Fast Path: PI794)	23
4.6.6 Benchmark Financial Ratio Maintenance (Fast Path: PI793)	23
4.6.7 Maintain Business Activity	24
5 Party Onboarding	25
5.1 Customer Onboarding (Fast Path: PI048)	25

5.1.1 Customer Onboarding: Individual	25
5.1.2 Customer Onboarding: Organization or Trust	26
5.2 Service Provider Onboarding (Fast Path: PI028)	27
6 Single Party View (Fast Path: PI100)	31
6.1 Landing Page (Party Search)	31
6.2 Landing Page (Detailed Customer View)	31
6.3 Snapshots	33
6.3.1 Contacts Details	33
6.3.2 Party Address	33
6.3.3 Manage Party Name	33
6.3.4 Party Images	33
6.3.5 Memos and Notes	34
6.4 Customer Requests	34
6.5 Profile: Individual	34
6.5.1 General Information	35
6.5.2 Identification	36
6.5.3 Employment	36
6.5.4 Financial Profile	36
6.5.5 Education	37
6.5.6 Blacklisting	37
6.5.7 Legal Reporting	37
6.5.8 Other Details	38
6.5.9 Consents	38
6.6 Profile: Organization	38
6.6.1 General Information	39
6.6.2 Identification	40

6.6.3 Financials	40
6.6.4 Blacklisting	40
6.6.5 Legal Reporting	40
6.6.6 Other Details	41
6.6.7 Consents	41
6.7 Profile: Trust	41
6.8 Relationships	43
6.8.1 Party to Party Relationship	44
6.8.2 Groups	47
6.8.3 Borrowing Entity	47
6.9 Holdings	48
6.10 Risk Indicators	52
6.11 Due Diligence	53
6.12 Credit Worthiness	54
6.12.1 Risk Score	55
6.12.2 Breaches	56
6.12.3 Bureau Report	57
6.13 Credit Exposure	57
6.14 Notifications	57
6.15 Calendar	58
6.16 Documents	58
7 Broker and Introducer Status Modification	59
8 Associated Party	61
9 Enquiry and Party Search	63
9.1 Basic Search	63
9.2 Advanced Search	65

10 Data Privacy and Security	67
11 Core Components	69
11.1 Core Entity Services	69
11.1.1 Calendar Services	69
11.1.2 Currency Services	70
11.1.3 Address Taskflow	70
11.1.4 Questionnaire Framework	70
11.2 Multi Entity Multi Branding	71
11.3 Alerts	72
11.4 Content (Document Management System)	73
11.4.1 Document Type Definition	73
11.4.2 Document Policy	73
11.4.3 Interface with Third Party Systems	73
11.4.4 Document Checklists	73
11.4.5 Regeneration and Resending of Documents	74
11.4.6 Acceptance and Execution of Documents	74
11.4.7 Document Search and Upload	74
11.4.8 Document Upload by External System	74
11.4.9 Services to Support Digital Channel	75
11.4.10 Stitching of Documents	75
11.5 Rule Author	75
11.6 Security Management System (SMS)	76
11.6.1 Security	76
11.6.1.1 Set Up User Roles and Entitlement Policies	76
11.6.1.2 Transaction Blackout Configuration	77
11.6.1.3 Origination Application Tracker Entitlements	77

11.6.2 Approvals	77
11.6.2.1 Matrix Based Authorization	79
11.6.2.1.1 Pricing Approval Negotiations	79
11.6.2.1.2 Credit Approval Negotiations	79
11.6.2.1.3 Collateral Processing Approvals	79
11.6.2.1.4 Transaction Limit Checks	80
11.6.2.1.5 Cancel Pending Approval Request	80
11.6.2.1.6 Approval Process Tracking	80
12 Interface with other Master Data Management	81

Preface

Oracle Banking Party Management enables banks to move from product-centric to customer-centric services. Banks can consider deploying Oracle Banking Party Management both as an independent standalone project and as a starting point for a broader progressive modernization program. The solution is built using standard enterprise components, provides efficient process automation, and is available on premise, on the cloud or through a hybrid model.

This preface contains the following topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

Audience

This guide is intended for the users of Oracle Banking Party Management.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/us/corporate/accessibility/index.html>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/us/corporate/accessibility/support/index.html#info> or visit <http://www.oracle.com/us/corporate/accessibility/support/index.html#trs> if you are hearing impaired.

Related Documents

For more information, see the following documentation:

- For installation and configuration information, see the Oracle Banking Party Management Installation Guide - Silent Installation.
- For a comprehensive overview of security, see the Oracle Banking Party Management Security Guide.
- For the complete list of Oracle Banking licensed products and the third-party licenses included with the license, see the Oracle Banking Party Management Licensing Guide.
- For information related to setting up a bank or a branch, and other operational and administrative functions, see the Oracle Banking Party Management Administrator Guide.
- For information related to customization and extension, see the Oracle Banking Party Management Extensibility Guide for Host, SOA, and UI.

Conventions

The following text conventions are used in this document:

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

1 Overview

Oracle Banking Party Management is a comprehensive solution from Oracle Banking products which provides an end to end party onboarding and servicing capability. It can also capture and maintain financials for different party types. Oracle Banking Party Management manages onboarding and all the servicing aspects of parties like Customer, Member, Affiliates and Service providers.

The party onboarding can be done through party onboarding standalone page. A deduplication check is performed on the parties to avoid duplicate party creation and once the party is on boarded, due diligence process is either triggered and completed by the user manually or initiated in the system automatically. Any update to the captured data or a fresh capture of data is supported through Single Party View page. Additionally, other servicing activities are also performed.

2 Party Bank Policy (Fast Path: PI314)

Party Bank Policy (Fast Path: PI314) is a maintenance helps a bank to define the various parameters and policies within which the party onboarding and servicing takes place. The bank level parameters for party is maintained here and is explained in this section. Configuration of party bank policy must be done as part of day zero configurations.

The functionality related to task flows pertaining to party module is explained below:

- **Resident Stability:** This criterion is used during Party Onboarding and the Party Address servicing pages. It indicates the minimum number of months a party needs to stay in a particular address, else capturing of Previous Home Address is mandatory. The number of months captured here are compared with Living Since field for Individuals and Occupying Since field for Trusts and Organizations to determine whether previous address is required or not. This field is validated during onboarding of all the roles, that is for customers, affiliates, and guarantors.
- **Minor - Major transition:** In certain countries, minors are granted limited rights after attaining a certain age even before they attain the age of majority as defined by law. Hence, Oracle Banking Party Management supports maintaining two Minor statuses in the system mainly, Minor and Operational Major. Bank can grant limited rights to children who have attained the age of Operational Major. For example, View Only access over internet banking is given to children on attaining the age of 14, and transaction access on attaining full majority at 18. Separate set of parameters are maintained in the system for these age groups.
 - The transition from minor to major in case of an Individual is automatic.
 - The date of birth is passed to the modules to calculate the date on which the party becomes major.
 - Party provides the service to account opening to check the legal or major operational age defined here, to determine the date for transition.
 - If the date of birth is modified, party informs the modules regarding the change in the date of birth. The onus of recalculating the date of transition to major status and logging the even in the batch lies with the respective modules.
- **Legal Major Age:** This is the age the attainment of which gives full legal rights to the party as per the law of the land. Based on the number of years input in this field, system calculates the date on which the party can attain majority. This date is stored in the system. The batch process of this date which performs minor to major transition picks up the party ID and change its status accordingly.
- **Operational Major:** This check box indicates whether bank wishes to utilize the Operational Major functionality. Refer the above explanation, to understand the meaning of Operational Major. If this check box is selected, then the additional fields where parameters for operational major are maintained are enabled.
- **Operational Major Age:** Here, the user captures the number of years completed which considers the party to be an operational major. Refer the above explanation, to understand the meaning of Operational Major.

-
- **Restricted Minor Maintenance:** This taskflow is the default one for capturing access right parameters for minors.
 - **Unrestricted Minor Maintenance:** This taskflow applies to the party's rights when the party is an Operational Major.
 - **Employment Stability:** This field denotes the minimum number of months for which employment and financial details of the individual borrowers should be mandatorily captured.
 - **Relationship Manager for a group:** A group of relationship manager who acts as the RM's for groups in Oracle Banking Party Management is created in OID. The name of the group is an input field, which picks the list of the RM's that can be linked to groups. This list is displayed under the drop-down for RM's when the groups is being maintained.
 - **Financial Year for a party:** The following fields will be maintained in party bank policy to define the financial year applicable for a party (In certain cases this is different from the financial year followed by bank). The start date, end date, start month, and end month for financial year is captured. The system validates that the total period of the financial year is equal to 12 months.
 - **Due Diligence Parameters:** Banks conduct many due diligence checks to confirm the authenticity of a party before onboarding a party. Few banks also revise their due diligence policy at regular intervals and wish to obtain the checks conducted at regular intervals for the customer. The parameters is used to configure each of the due diligence types, to configure the applicable identity verification components, their respective expiry applicability, and the expiry period. These is later used while performing checks.
 - **Parameter to store lead days for expiry of verification types:** This parameter stores the lead days for expiry tracking purpose. This parameter is used by the system to generate an alert and/or an advice to be sent to the party intimating that the verification type (for example: KYC) is about to expire. This gives sufficient time to the party to visit the bank with necessary documents and re-confirm the verification type (for example: KYC).
 - **Rule to resolve manager for Broker or Introducer:** Place holder will be provided to link the rules which will resolve to create a list of managers who can be linked to broker or introducer for each business group. The rules are authored using rule author and is attached here. The rules are executed while onboarding an Individual broker or introducer to resolve the list of managers from whom a manager can be linked to the broker or introducer for the specific business group.
 - **Rule to resolve the list of RM's for each party type is also available under the rule maintenances.** The rule is resolved to pull the list of RM's for each party type from OID. The specific list of RM pulled from OID is available under the drop-down RM, when the party is being onboarded.
 - **Rule to resolve the mode of due diligence to be performed for the party according to party role, party type, and so on is also attached in party bank policy.**

The facts that is used to create the rule for due diligence for each identity verification are:

- Event Code
- Party Type
- Party Role
- Relationship (if party role is Affiliate)

Output is:

- Electronic: Yes or No
- Manual: Yes or No

3 Bank Policy

Certain bank level parameters referred by party, which are maintained here are explained in this section:

The functionality related to taskflows pertaining to Party module is explained below:

Broker and Introducer parameters: This taskflow captures some parameters pertaining to Brokers and Introducers.

- If the Enable Capture of Commission check box is selected, then the Interface with External Commission System check box is enabled. It should be set as Yes, if the bank derives the commission from an external commission system, else it should be deselected.
- Broker or Introducer IDs: Every broker or introducer is onboarded in the system as a party and assigned a Party ID. In addition, they are assigned separate SPIDs (Service Provider IDs) which is used to map them with other external systems where such host systems of such service providers are maintained.
- Bank also decides whether Broker and Introducer IDs should be generated automatically or be manual input.
 - The option once chosen cannot be changed, except before generation of the first broker or introducer ID.
 - In case of automatic generation of IDs, bank provides the mask in which the IDs are generated.
 - The IDs are always unique. In case of manual IDs, the system validates that ID input by the user is unique, else it displays an error.

4 Party Maintenances

The various maintenance pages in Party module are explained below:

4.1 Relationship Maintenance (Fast Path: PI020)

The functionality of the Relationship Maintenance page is as follows:

- The page is used to define relationships as a day zero activity by the bank.
- This is one-time activity. Addition of new relationships later is possible, but such occasions are less. Relationships once created cannot be closed or deleted.
- These relationships is used to map two parties or to map parties to accounts. The mapping is done through different pages, Party to Party and Party to Account.
- Once the mapping is done, it can be exploited by individual modules to offer enhanced functionalities in cross selling, relationship management, exposure tracking, income sharing, pricing, and so on.
- The Relationship Maintenance page also defines specific attributes of each relation, such as those pertaining to facilities, access, sharing, and so on. These attributes are used by the application to determine the defaults at transaction level, as well as to grant or deny permissions. For example, if the relation Authorized Signatory has the Alert Allowed check box as selected, then the alerts are sent to this relation (provided they are further granted down the line at account level and are available for the event). However, if the check box is not selected, then the alerts are not sent to this relation at all.

4.2 Relationship Rules Definition (Fast Path: PI021)

The purpose of this page is to define the mandatory relationships to be on boarded for a party. Such requirements occur because banks may have differential policies on onboarding and KYC when customers are on boarded, based on party type or some other related factors such as constitution, age, and so on. Some examples of this are given below:

Examples:

- If Party Type is Organization, then onboard minimum one Owner and one Administrator.
- If Party Type is Organization and Constitution is Company, then onboard minimum one Director or Promoter (as Owner) and one Authorized Signatory (as Administrator).
- If Party Type is Organization and Constitution is Partnership Firm, then onboard minimum two Partners (as Owner) and one Authorized Signatory (as Administrator).
- If Party Type is Individual and Party Age < 12, then onboard Guardian as Mandatory.

Rules such as the above can be set up using the Rule Author (Fast Path: RL001) page. When the party is onboarded, based on the Party Type, Constitution, and so on, the system forces the user to onboard the required number and type of affiliates. This ensures automatic compliance of customer onboarding rules by the user.

Rules are created for a Party Type - Effective Date combination and internally the system creates the version numbers and retain all the rules. During onboarding, based on the system date of the application, the appropriate rule is enforced.

The system also creates a rule ID and rule name internally. It is not visible to the user.

The domain name and domain category is stamped as Banking and Party respectively. This is not visible to the user.

4.3 Role Master (Fast Path: PI014)

The list of roles available in the system are primarily factory shipped and cannot be changed. The Role Master page provides a front end to visualize the list of roles available and make modifications. Here, only the Role Description and the eligible Party Type can be modified.

No changes are ordinarily expected to be made through this page after the day zero configuration.

4.4 Bureau Maintenance (Fast Path: PI099)

Credit Bureaus are organizations that provide information about individuals and businesses' creditworthiness to lenders such as banks. This helps lenders to assess credit risk of the customer appropriately and take suitable decisions on lending proposals. Banks may decline proposals from applicants with less favorable credit history or may price loans to them differently to account for differential risk.

Debit bureaus are data warehouses with decision support capabilities to help financial service companies make debit decisions, like whether to let a customer open a checking account. This Bureau Maintenance page is used to maintain the names of such credit and debit bureaus, which the bank deals with along with certain other details pertaining to those bureaus.

The first section of the page is used to capture the bureau details and the address details of the bureau. The subsequent sections captures the different services provided by each bureau and for each service the parameters with effect from a particular date.

Note

To set up fully functional bureau maintenance, an interface with an external credit rating system/debit bureau is necessary. Maintenance of some of the fields given here would depend on the external system and the interface with it, which would be part of consulting activity.

4.5 Manage Groups (Fast Path: PI024)

Group could be termed as a group of customers (or members) who are related or associated to each other or any of the members of the group.

A customer can be part of many groups as the relation of a party with certain other parties will differ. There can be certain groups where a party is part due to business reasons. For example: In one group as the party is the major distributor of goods for another party.

The same party can have personal relations and can be in another group due to the virtue of this personal relation. The decision on whether the party has to be considered for credit decisioning and for viewing exposure is decided at the submission level.

- In order to add members to the group, the Members Details section is provided. The user can search for the party to be added to the group as group member using the basic or advanced party search and add the party as group member by clicking on the Add button.
- All the memos for the party is displayed while the party is being added as a group member.
- If a party is marked as deceased, Memo is shown to the user before adding the party as a group member.
- When a blacklisted party is being added to the group, then the system displays a warning message and continues if the user wishes to proceed.
- All the group members added is displayed in multiple rows.

4.6 Financial Maintenance

The suggested order of maintenances before initiating financial capture in standalone flow is as follows:

4.6.1 Financial Category Maintenance (Fast Path: PI027)

- Multiple financial categories can be maintained using this page. Existing category codes is available as seed data.
- Each category ID will have unique three digit alpha numeric code name and is input field by the user (For example: Current asset is defined as CASA).
- Category code maintained here is linked to the financial parameter code through Financial Parameter Codes (Fast Path: PI791) page.
- Category codes is not allowed to be deleted as the same impacts the existing functionality. Hence, the option to delete the category codes is not be provided as part of the maintenance page.

4.6.2 Financial Nature Maintenance (Fast Path: PI790)

- A front end maintenance is provided for the user to maintain financial nature.
- Financial parameter linked to nature as business plan is used in the Business Plan Template Maintenance (Fast Path: PI792) page to link financial parameter code to a Business Plan. For example: Crop income defined as parameter code is linked to financial nature as Business Plan.
- Financial nature is not allowed to be deleted as the same impacts the existing functionality. Hence, the option to delete the financial nature is not be provided as part of the maintenance page.

4.6.3 Financial Parameter Codes (Fast Path: PI791)

A parameter code constitutes of the below attributes:

- Financial Parameter Code: This is a unique identifier which uniquely identifies the financial parameter. This number is system generated. Numbering method is defined in the above section.
- Financial Parameter Name: The name of the financial parameter. Parameter names are individual elements which comprise of the financial statement. When financial details are captured, the values are entered by the user against these parameters. For example: Cash in Hand, Inventory, Rent, and so on.

- **Base Type:** It identifies a part of the statement that is currently being defined. The list of base types are factory shipped. All the base types that are available appears in the list.
- **Category:** Within each of the base types given above, data is consolidated under multiple categories which represent elements of similar nature or belonging to the same financial aspect. A list of such categories are made available as seed data, but it is possible for the bank to add its own categories through separate maintenance.
- **Value Type:** This field indicates how the value of the code is populated in the financial statement.
- **Nature:** This field is used to define certain additional parameters which the banker needs to capture while capturing the value for that particular financial parameter. For example, for the nature loan, which is a liability in the balance sheet for the borrower, the banker can define fields like repayment amount, frequency, which the banker uses in further assessment.
- **Include for DSO:** This check box indicates if the parameter code is to be used in Debt Service Obligation computation. If this check box is selected, then this parameter is available for linkage in the Debt Service template.
- **Include for Statement of Equity:** This option indicates if the parameter code is used in the Statement of Equity template. If this option is selected, then this parameter is available in the Statement of Equity template.
- **Monthly split required:** This check box is used to capture preference if this field value is required to be split into monthly values during financial capture. If this check box is selected, then in financial capture, provision to capture monthly split figures is not available.
- **Mandatory Value:** This field is to specify whether Original amount, Current Outstanding, or both amounts needs to be mandatorily captured for the liability parameters and to be used.
- **Borrowing Power Calculator Use:** This field is to specify whether Original amount and Current Outstanding needs to be captured for the liability parameters and to be used for borrowing power.
- **Ownership Percentage:** This field determines whether the ownership percentage is applicable or not for a financial parameter code. If this is not selected, then the percentage field is defaulted to NA.
- **Foreign Sources:** This field determines whether the parameter code that is being maintained is from a foreign source.

4.6.4 Financial Statement Template (Fast Path: PI794)

When a statement template is defined, the user chooses from the following options:

- **Statement Type:** The user captures the type of the statement being created, for example: Balance Sheet. This list is factory shipped and consists of the following:
 - Balance Sheet
 - Profit & Loss Account
 - Cash Forecast
 - Financial Ratios
 - Debt Servicing template
 - Statement of Equity
 - Net Customer Position

Only one Cash Forecast statement is allowed to be maintained. User can edit the statement, and also add or delete the parameter codes as required. Further all the parameter codes in Cash Forecast is non-mandatory.

Business plan is a separate maintenance and is not be a part of the Statement template. However, financial parameter values in business plan defaults to the Cash Forecast statement. Multiple business plans are maintained as per the activity and linked to the Cash Forecast statement.

Debt servicing template is a separate statement template to arrive at the amount available for servicing. This statement template is defaulted directly in the financial analysis and is not a part of the financial template.

Statement of Equity is separate statement template to explain the changes in a firm's retained earning's over the reporting period. The statement breaks down the changes in owner's interest in the firm and in the application of retained profit or surplus from one accounting period to the next. The parameters which form part of this statement include profits and loss from operations, dividends paid, issue or redemption of stock, and any other items charged or credited to the retained earnings.

- **Statement Generation:** User clicks the Review Statement button at the bottom of the page. Then the system generates the statement internally and displays it to the user for confirmation. If user is satisfied with the configuration, user clicks on the Save button to confirm the creation of the statement.

4.6.5 Financial Statement Template (Fast Path: PI794)

A financial template is used to determine the type of financial information being captured for a party. A template contains one or more financial parameters belonging to the respective type of information, that is Asset, Liability, Income, and Expense.

Financial Template is defined based on the party type that is, Individual, Organization, and Trust. The financial template definition needs the factory shipped financial parameters for individual, organization, and trust to be configured. During template definition, the user can select asset, liability, income, and expense items based on the financial parameters defined within the system.

In case of an Individual party type, the template is configured based on the employment type.

The employment type has the following key list of values:

- Salaried
- Self Employed
- Salaried and Self Employed
- Others

Multiple financial templates are maintained for all party types Individual, Organization, and Trust.

4.6.6 Benchmark Financial Ratio Maintenance (Fast Path: PI793)

- Benchmark financial ratios for an Industry are primarily used to compare party financial ratios or measure party performance operating in the similar Industry. The party herein refers to an Individual, Organization, and Trust whose key financial ratios are analyzed and compared with benchmark financial ratios of the same industry type.

- In order to support the analysis of the financial ratios, a front end maintenance page for maintaining benchmark financial ratios is provided to the user. The values maintained for the industry type is displayed during the financial spreading.
- Apart from benchmark values for the Industry, benchmark value for bank is maintained along with the industry benchmark values. This enables the banks to maintain separate bench mark values.

Benchmark financial ratio is defaulted and used in financial spreading. Industry type maintained as seed data is available as a pick list and user have an option to link the industry at any level. This maintenance allows the user to maintain benchmark value for any number of industry types. For example, the user may choose to maintain benchmark value for current ratio for multiple Industries.

4.6.7 Maintain Business Activity

User will define business plan as separate maintenance and consists of financial parameters and business activity parameters. Business plan is linked to cash forecast statement and there is only one cash forecast statement to which multiple business plans can be linked. The approach to maintenance of business plan is detailed here below:

- Business plan is defined to support single business activity. For example, for business activity like, Crop, Livestock, Poultry, Wool, and so on.
- Financial parameter codes linked to financial nature as Business Plan is available in the pick list in the business plan maintenance page.
- Activity parameters are captured as input and totals (expression) are linked to financial parameter code. For financial parameter crop income, Activity Parameters Area, Yield, Price, Share %, and the total (area* yield* price*share %) are applicable.
- The values captured in the business plan for each of the financial parameter code is defaulted to the cash forecast statement.
- Multiple templates for business plan are maintained by the user based on the business requirement and attached to the cash forecast statement.
- The capture of business plan is not mandatory. The user may choose to manually capture the details in the cash forecast statement.
- In addition to the above, the user can call the taskflow of the nature (additional details) maintenance and capture additional details for the parameter in the business plan maintenance page itself. For example, if the Non Business Income is required to be captured with parameter as Income, then the same can be defined in the parameter maintenance page.

5 Party Onboarding

Customer onboarding involves capture of personal details of the applicant and generating a Party ID for the user. During the process, certain other steps such as triggering KYC, performing deduplication, and so on are also performed. When onboarding is complete, Party ID is generated and the role as Customer is assigned to the ID.

5.1 Customer Onboarding (Fast Path: PI048)

The steps that need to be followed to complete the onboarding process are mentioned below:

- When onboarding is done through standalone page, user has to first select the party role as Member or Customer. By default Member is selected and Customer can be chosen to proceed.
- User also needs to select the Party type of the customer being onboarded, the party types are:
 - Individual: This party type corresponds to a party who is a natural biological person.
 - Organization: This party type is used to capture all such non-individual entities, which may broadly be classified as commercial in nature.
 - Trust: This party type is used to classify all the non-individual entities, which are registered as trust in their respective jurisdictions.
- For member onboarding, once the party role is selected as Member and the required party type is selected, very minimal data that are Name and Date of Birth are mandatory to be captured for the onboarding process to be completed. A party ID is created once the onboarding process is completed.

5.1.1 Customer Onboarding: Individual

- While onboarding a Customer, once the party role is selected as Customer and the required party type (Party Type: Individual) is selected, then the user is prompted to capture the below details before the onboarding process is completed:
 - Primary Details: Refers to Legal Name, Alternate Name, Basics Details, Residential Address, Work Address; Services Details that needs to be captured.
 - Contact Details: Refers to the contact point Phone or Electronic Address at which the party can be contacted.
 - Additional Details: Refers to Anti-Money Laundering Characteristics Details, Marketing Question, Documents Receiving Preference, Consents Details that need to be captured.
 - Identification Details: Consists of the capture of Tax identification details and other identification details. Additionally, Tax residency details of other country (other than primary country of citizenship) is captured.
 - Employment Details: Employment details can be captured as part of this tab.
 - Roles/Relationships: Affiliates like Administrator can be added from this tab. These can be a new or existing party in the system.

- **Checking Party Duplication:** At any point during the details capture or once the same is done the deduplication process can be invoked by clicking on this button (if not clicked, then checking of party duplication happens automatically on Save and Submit). Based on the details of the party captured by the user, deduplication is performed and possible duplicate records are identified and displayed by the system to the user. The user then has to operationally decide whether the person being onboarded exists in any of the matched records or is a new person or an entity. System provides the user an option to select one of the matched records, or override and proceed with the onboarding as planned.
- Once the details are captured and the party is onboarded, a party ID is assigned to the party.
- **Due Diligence:** Due diligence rules are maintained in the Define Party Bank policy (Fast Path: PI314) page. System sends the business unit, party role and party type to the rules definition and determines which verifications are due diligence checks and the linked identity. Based on the day zero parameter, due diligence is either set as Auto or User Initiated. In case it is User Initiated, then the due diligence of the party is triggered and processed once the party onboarding is completed.

5.1.2 Customer Onboarding: Organization or Trust

- **Customer Onboarding (Party Type: Organization or Trust)**
 - **Primary Details:** Refers to details like Legal Name, Identification Details, Constitution, Establishment Date, Registered Address that needs to be captured.
 - **Contact Details:** Refers to the contact point Phone or Electronic Address at which the party can be contacted.
 - **Additional Details:** Refers to the details like Anti-Money Laundering Characteristics details, Consents details that needs to be captured.
 - **Identification Details:** Consists of the capture of tax identification details and other identification details. Additionally, tax residency details of other country (other than primary country) can be captured.
 - **Roles/Relationships:** Affiliates like Administrator, Owner or Beneficiary (only for party type as Trust) can be added from this section. These can be a new or existing party in the system.
 - **Checking Party Duplication:** At any point during the details capture or once the same is done the deduplication process can be invoked by clicking on this button (if not clicked, then checking of party duplication happens automatically on Save and Submit). Based on the details of the party captured by the user, deduplication check is performed and possible duplicate records are identified and displayed by the system. The user then has to operationally decide whether the person being onboarded exists in any of the matched records or is a new person or an entity. System allows user an option to select one of the matched records, or override and proceed with the onboarding as planned.
 - Once the details are captured and the party is onboarded, a party ID is assigned to the party.
 - **Due Diligence:** Due diligence rules are maintained in the Define Party Bank policy (Fast Path: PI314) page. System sends the business unit, party role and party type to the rules definition and determines which verifications are due diligence checks and the linked identity. Based on the day zero parameter, due diligence is either set as Auto or User Initiated. In case it is User Initiated, then the due diligence of the party is triggered and processed once the party onboarding is completed.

5.2 Service Provider Onboarding (Fast Path: PI028)

Details of various individuals the bank deals with, besides its customers, also needs to be captured into the system. All such individuals are onboarded and assigned different roles based on the nature of their dealing with the bank. They are collectively called as Service Providers.

The process of onboarding a service provider is similar to the process of onboarding a customer from the standalone page. The extent of data capture can be slightly less than in the case of a customer, while certain additional details which are specific to that particular role can be captured. In this section, only the role specific details are explained, while for personal details such as Name, Date of Birth, Address, and so on, the reader can refer to the Customer Onboarding (Fast Path: PI048) page since the functionality, validations, and business rules are the same in both the cases.

Note

The Service Provider Onboarding page are only for onboarding the Service Providers (Fast Path: PI028) (Individual, Organization or Trust). This page cannot be used to onboard parties in other roles such as Affiliates or Guarantors.

The various Service Provider roles that can be onboarded are mentioned below:

- **Broker:** An individual broker is linked to the Business Group (it is a specific group of products configured within Oracle Banking Party Management). Hence, while onboarding an individual broker, there are certain additional role details and business group specific details that needs to be captured. The role specific details that are captured for the broker are:
 - **Broker ID:** In case of a broker, the system generates a broker ID to uniquely identify the broker. The broker ID is over and above the party ID which is generated for the broker.
 - **Parent Broker or an Agency ID:** Brokers may be very large in number with some of them sub-brokers working under a parent broker. The ID of such a parent broker is captured in the system. For an individual sub-broker, the parent can be another individual or organization.
 - **Business Group Specific Details:** The business group specific details for a broker is captured for each business group the broker is linked to.
 - **Home Business Unit:** The home business unit of the user's login branch (top right hand corner of the page) is defaulted as the home business unit for the broker being onboarded. The user can change it to any other available business unit.
 - **Deduplication:** Upon submit of the page, deduplication is performed as in case of individual onboarding.
 - **ID generation:** Two types of IDs are generated upon submit that are, the Party ID of the Broker (Role = Broker) and the Broker ID (if Broker ID generation = Automatic, as maintained in the Define Party Bank Policy page).
- **Document Verification Agency:** It is predominantly expected to be an Organization, though Oracle Banking Party Management supports the role to be assigned to an Individual. In case it is an individual, the details of the individual captured during onboarding are the same as in case of an individual customer, though it is fewer. Other than the Primary, Contact, and Identification details, Role details mainly Vat Number, Trade Association, Payable Currency, Tax Scheme, Payment Type, and Contract details are captured. When the Document Verification Agency is on boarded,

upon successful submit of the page, the system generates a Party ID and assigns the role of Document Verification Agency.

- **Introducer:** The functionality with regard to Introducer onboarding is similar to onboarding process of a Broker. Only the following points are different:
 - **Introducer ID:** In case of an introducer, the system generates an introducer ID to uniquely identify the introducer. The introducer ID is over and above the party ID which is generated for the introducer.
 - **Parent Introducer or Agency ID:** Introducers are very large in number with some of them working under a parent introducer. The ID of such a parent introducer is captured in the system. For an individual, the parent can be another individual or organization.
 - **Introducer Status:** It can be any of the following: Active, Inactive, Deceased, and Terminated.
 - **ID Generation:** Two types of IDs are generated on submit that are, the Party ID of the introducer (Role = Introducer) and the Introducer ID (if Introducer ID generation = Automatic).
- **KYC Agency:** The KYC agency is predominantly expected to be an Organization, though Oracle Banking Party Management supports the role to be assigned to an Individual. In case of an individual, the details of the individual captured during onboarding are the same as in case of an individual customer, though fewer. Other than the Primary, Contact, Identification details, Role details, the details such as Vat Number, Trade Association, Payable Currency, Tax Scheme, Payment Type, and Contract details are also captured. When the KYC agency is onboarded, upon successful submit of the page, system generates a party ID and assigns the role of KYC Agency.
- **Title Search Agent:** The title search agent could be an Organization or an Individual. In case it is an individual, the details of the individual captured during onboarding are the same as in case of an individual customer, though fewer. Other than the Primary, Contact, and Identification details, Role details, the details such as Vat Number, Trade Association, Payable Currency, Tax Scheme, Payment Type, and Contract details are also captured. When the title search agent is onboarded, on successful submit of the page, the system generates a party ID and assigns the role of Title Search Agent.
- **Valuer:** The valuer could be an Individual, Organization or Trust. In case it is an individual, the details of the individual captured during onboarding are the same as in case of an individual customer, though fewer. Other than the Primary, Contact, and Identification details, Role details, the details such as Valuation Type, Environment Risk Assessment Eligibility, Accredited, Certified Licensed, Contract details are also captured. When a valuer is onboarded, on successful submit of the page, the system generates a party ID and assigns the role of Valuer.
- **Vendor:** In case the vendor is an individual, the details of the individual captured during onboarding are the same as in case of an individual customer, though fewer. Other than the Primary, Contact, and Identification details, Role details, the details such as Vat Number, Trade Association, Payable Currency, Tax Scheme, Payment Type, and Contract details are also captured. When the vendor is onboarded, on successful submit of the page, the system generates a party ID and assigns the role of Vendor.
- **Settlement Agent:** The settlement agent is an Individual or Organization. In case the settlement agent is an individual, the details of the individual captured during onboarding are the same as in case of an individual customer, though fewer. Other than the Primary, Contact, and Identification details, Role details like Settlement Agent details such as Contract Start Date, End Date, and Description are also

captured. When the settlement agent is onboarded, on successful submit of the page, the system generates a party ID and assigns the role of Settlement Agent.

6 Single Party View (Fast Path: PI100)

6.1 Landing Page (Party Search)

- The landing page of the Single Party View menu is a Party Search page. From this menu, the user can view party details of a party at a time. In case, the context party needs to be changed, then it can be done from this page or by clicking the available Party Search panel drawer.

Note

The Party Search panel drawer is available in all the pages of the Single Party View menu including all child pages. The user can click this panel drawer item at any time, select the party, and click on the Enter button.

- This menu can be used to view, add or edit details of all the parties maintained in the Party module that is, parties in the role of Customer, Co signor, or Guarantor as well as those in other roles such as Affiliate, Broker, Introducer, Valuer, and so on.
- User can perform two types of searches: Basic Search and Advanced Search.
 - Basic Search allows the user to search for party details based on some selected criteria such as Party Name, Party ID, Email ID, or Account Number.
 - The Advanced Search is a common taskflow. The system invokes the Party Search where the user wants to search based on Party Role or Party Type.

6.2 Landing Page (Detailed Customer View)

- Once the required party is selected, the system loads the Single Party View page for detailed customer view. This page is divided into multiple widgets and panel drawer items.
- This is a read only page. On navigating to the child pages, they are read only by default and allows to update or delete, and so on...
- The below table shows the various widgets of Single Party View menu:

Table 6–1 Widgets of Single Party View

S.No.	Widget	Child Pages
1	Snapshots	Contacts
		Address
		Party Name
		Memos and Notes
		Party Image
2	Customer Requests	Customer Requests

S.No.	Widget	Child Pages
		Application Tracker
3	Profile - Individual	General Information
		Identification
		Employment
		Financials
		Education
		Black Listing
		Legal Reporting
		Other Details
		Consents
4	Profile - Organization and Trust	General Information
		Identification
		Financials
		Black Listing
		Legal Reporting
		Other Details
		Consents
5	Relationships	P2P Relationships
		Groups
		Borrowing Entities
6	Notifications	Notifications
7	Holdings	Holdings
		P2A Relationship
8	Risk Indicators	Risk Indicators
9	Due Diligence	Due Diligence
10	Credit Worthiness	Risk Score
		Breaches
		Bureau Reports
		Credit Exposure
11	Calendar	Outbound Documents

S.No.	Widget	Child Pages
12	Documents	Inbound Documents
		Outbound Documents

- The functionalities related to each of these widgets and their child page have been detailed in the topics below.

6.3 Snapshots

Snapshots is a child page of the Party Summary widget. From the Party Summary page, the user clicks on the Maximize icon, and the Snapshots page appears.

The Snapshots child page is broken into following sections:

- Contacts Details
- Party Address
- Manage Party Name
- Party Images
- Memos and Notes

The details of each sections are explained below.

6.3.1 Contacts Details

A bank uses various communication platforms to communicate with its customers, such as phone, email, postal mail, social media, and so on. The contact section captures details of the parties at which they can be reached. It also stores customer's preferences in this regard and identifies default communication modes, if any.

6.3.2 Party Address

As part of party onboarding, address of the party is mandatorily captured. This address is used to perform the party's KYC, as well as used to send physical communications such as account statements, marketing mailers, and so on.

6.3.3 Manage Party Name

- Oracle Banking Party Management supports capture of multiple types of names for a party.
- The Manage Party Name section allows the user to capture, change the name for the party, and maintain additional names.

6.3.4 Party Images

- The Party Images section allows the user to upload image files pertaining to the party such as party photographs and signatures.

- The type of file extensions that can be uploaded are, .bmp, .gif, .png, .jpg, .jpeg. The maximum file size allowed is one MB.

6.3.5 Memos and Notes

- Memos and Notes provide page level alerts or notifications to the users performing transactions.
- This section allows the user to capture memos and notes for a particular party. This is a maintenance section. The memos and notes maintained here is used by individual modules to generate alerts.

6.4 Customer Requests

- This widget is available in the landing page below the Relationship widget.
- Following customer request is supported:
 - Cheque book request for transaction accounts
 - Track request for the applications in-progress
- This widget is applicable to all the party types. In case there is no active customer request, then the system shows a message “No pending customer requests” in this section.

Note

The details displayed in this widget are fetched from an external module. Hence, for standalone, the party details are not displayed, but product hooks are provided to fetch the details from the module and display the same.

6.5 Profile: Individual

Party Profile widget stores general personal information about the party. Some of this information is captured at the time of onboarding itself and is available for viewing and update through this widget. In addition, the Profile widget makes several other fields available where additional information about the party are maintained.

Unless otherwise stated, the functionality described below applies to all the roles such as Customer, Service Provider, and Affiliates. By default, all the sections in the page are shown in Read mode with Update (Create and Update functionality are merged into Update) and Print buttons enabled. On click of the Update button, all the fields in this section becomes editable along with OK and Cancel button enabled (Update button is disabled and Print button is always enabled).

In case of Update mode, the user cannot navigate from one section to any other section in the same page or move to any other page without clicking the OK or Cancel button.

The Profile Widget displays the following details in the Summary page:

- Date of Birth
- Employment Type
- Role
- Home Branch
- Customer Since

- Last Activity on
- Relationship Manager

The Profile child page supports the following sections:

- General Information
- Identification Details
- Employment Details
- Financials Details
- Education Details
- Blacklisting Details
- Legal Reporting
- Other Details
- Consents

The details of each sections are explained in subsequent sections below.

6.5.1 General Information

The General Information page stores information about the Party. Some of the details captured during party onboarding are defaulted in this page and are available for viewing and modification. The details are mainly from the following taskflows:

- Primary Information
- Marketing Details

The General Information page is further divided into multiple sections as listed below:

- About: This section displays the basic personal information related to the party.
- Dependent Details: This section captures the details about the dependents of the party. This is an optional section.
- Role Details: This section captures the role specific details of the service providers. This section is applicable for Service Provider role and not for the Customer or Affiliate roles.
- Risk Rating Details (show or hide panel): This section captures the risk rating details of the party. This is an optional section.
- Physical Attributes (show or hide panel): This section captures the physical features of the party such as blood group, height, weight, and so on. These are purely data capture fields with no processing involved.
- Hobbies and Interest (show or hide panel): This section captures the personal interests of the party. These are pure data capture fields with no processing involved.

6.5.2 Identification

- The Identification section captures the various identification details of the party. The identification details captured during onboarding are populated here and are available for modification.
- The list of identification types are populated based on the seed data given by the bank during parameterization.
- In Update mode, user can capture, edit, or delete the identifications.
- A facility to view, delete, or upload documents are supported for both tax identification as well as other identification details.

6.5.3 Employment

- The Employment section allows to capture or maintain the employment details of the party. Capture of employment details can be done either during onboarding or from this section.
- The employment details have a linkage to capture party financials, which is explained in the Financials section later in this document.
- Employment details are relevant only for Individual party type.

6.5.4 Financial Profile

- The Financial section allows to capture or maintain the financial details of an Individual party.
- The financials template is available for the employment types like, salaried, self-employed, and for a combination of salaried and self employed.
- User has the option to select the template that needs to be captured for a party.
- In case of salaried employment type, the following details are captured:
 - Income
 - Expense
 - Assets
 - Liabilities
- Option to create financial linkages between the income, expense, assets, and liabilities are available.
- In addition to this the ability to view current position and net customer position of the party is also available.
- In case of self-employed, a financial template which consists of multiple statements can be selected and the data is captured. The financial template usually comprises of the following statements:
 - Balance Sheet
 - Profit and Loss
 - Financial Ratios
 - Statement of Equity

- In case of a party who has multiple employments (that is, salaried as well as self-employed), then the combination of template for salaried and self-employed are available to capture the salaried income, and the statements for self-employed income.
- Ability to spawn the financial capture as a separate human task.
- Ability to create a questionnaire for each template to answer the questions regarding inconsistencies in the financials that has been captured.

6.5.5 Education

- The Education section allows the banker to capture education details about the party. The education details fields are pure data capture fields with no processing involved.
- The list of values in the picklist for Qualification and Mode of Study is factory shipped. Additionally, the bank adds its own list during parameterization.
- By default, the existing details captured are shown in this page. The user can add, edit, or delete the education details.
- To add details, the user clicks the Add button, which creates a new row in the table. The qualification and mode of study is a picklist and is mandatory to capture, the rest of the fields are optional text fields which are to be entered manually.
- The existing records can be edited or deleted. On delete, the entire row is deleted. If required the user can add a new row. If edited, all the columns in the table for that particular row becomes editable.

6.5.6 Blacklisting

- A bank deals in various service providers who are onboarded in respective roles. Occasions may arise when a service provider is required to be blacklisted for some reasons. This section is used for this purpose.
- For service providers, this section can be used to blacklist, modify blacklisting details, and delete the blacklisted status.
- If a service provider is blacklisted, then the party is excluded from various picklists.
- This exclusion happens from the date captured in the Effective Date field.

6.5.7 Legal Reporting

- FATCA stands for Foreign Account Tax Compliance Act, a legislation enacted in the United States of America to combat offshore tax evasion and recoup federal tax revenues. The legislation is applicable to all the banks that hold accounts of American citizens and its non-compliance may attract penalties for the bank in its operations or investments in the United States.
- While FATCA compliance is typically handled through some other external application, Oracle Banking Party Management as the source core banking system is required to capture additional data elements required for compliance on behalf of the party.
- These data elements are captured through the Legal Reporting section in the Profile widget and are handed off to some external system for reporting and compliance.
- When tax residency country is selected as USA, then FATCA details are mandatory to be captured.
- FATCA details are mostly data capture fields and are not used anywhere in processing.

- Legal reporting details are captured only if the party role is Customer. This section appears on the Profile widget, if the party role is different.
- The expected functionality is to capture the data and hand it off to an external system, that handles the FATCA compliance for the bank.

6.5.8 Other Details

- The Other Details section captures details of the party like whether the party is exempted from cash transactions, whether the party is an insider of the bank, or related interest of the insider, and so on.
- CTR Details: A field to check whether CTR exemption is available, if this is selected then the date of exemption field becomes mandatory.
- Insider Details: Supports modification and inquiry of insider details.
 - The details captured during onboarding are displayed.
 - User can also view, add, edit, or delete insider details.
 - A party can be insider of bank or a party can be related interest of an insider.

6.5.9 Consents

- The Consent section allows the banker to capture the following details about the party:
 - Anti-Money Laundering characteristics
 - Marketing
 - Services- Access Channels
 - Documents
 - Consents
- Anti-money laundering characteristics like source of funds, source of wealth, and purpose of relationship are captured and updated.
- Access channels like internet banking, mobile banking, and phone banking are opted in from this section.
- The list of consent question values are factory shipped. Additionally, the bank adds its own list during parameterization.

6.6 Profile: Organization

Party Profile widget stores general information about the party. Some of this information is captured at the time of onboarding itself, and is available for viewing and updating. In addition, the Profile widget makes additional fields available where more information about the party are maintained.

Unless otherwise stated, the functionality described below applies to all the roles such as Customer, Service Provider, and Affiliates.

The Profile widget displays the following details in the Summary page:

- Constitution
- Role

- Home Branch
- Customer Since
- Last Activity on
- Established on
- Industry
- Country of Establishment
- Relationship Manager

All the details in this page are Read only. The user can use the Maximize button provided in right top end corner to navigate to the Profile child page, which allows to view and edit of profile information.

The Profile child page supports the following tabs:

- General Information
- Identification
- Financials
- Blacklisting
- Legal Reporting
- Other Details
- Consents

The details of each sections are explained in detail in subsequent sections below. All the existing functionalities continues to exist, unless specifically mentioned in this document.

6.6.1 General Information

- The General Information page stores information about the party. Some of the details captured during party onboarding are defaulted in this page and are available for view and modification.
- All the fields are pure data capture fields which are populated from the onboarding page or captured here in the Update mode and are available for modification.
- The General Information page is further divided into multiple sections as listed below:
 - Organization Details
 - Other Details
 - Role Details
 - Risk Rating Details (show or hide panel)
 - Shareholders Details (show or hide panel)
 - Scrip Details (show or hide panel)
 - Direct Entry Identification Details

6.6.2 Identification

- The functionality, fields, and validations are same as for Individual party type.
- Only the Other Identification Type seed data is different for organization.

6.6.3 Financials

- The Financial section allows to capture and maintain the financial details .
- Oracle Banking Party Management allows the bank to define parameters (such as salary, home loan, general living expenses, and so on) under different categories (such as income, expense, and so on). For defining business statements, applicable parameters are grouped together to form statements such as balance sheet or profit and loss.
- Ability to capture the following statements:
 - Balance Sheet
 - Profit and Loss
 - Financial Ratios
 - Statement of Equity
 - Cash Forecast
 - Business Plan
- Multiple templates for the same statement type are created. For business customers, these statements are clubbed together under a financial template. Bank can specify which statements are to be added together.
- The applicable templates for a party are provided as part of a drop-down and the user can select the template to be filled in.
- A bank can spawn off the financial capture as separate human task to back office.
- Oracle Banking Party Management allows the bank to perform bulk upload of the financial documents in the financial profile.
- While maintaining a template, Oracle Banking Party Management has provided an option to link a questionnaire. The questionnaire which is linked to template are initiated when financials is being captured for a party. This enables the banker to use certain questions regarding the customer financials.

6.6.4 Blacklisting

- The functionality, fields, and validations are same as Individual party type.

6.6.5 Legal Reporting

- The functionality, fields, and validations are same as Individual party type, except the following:
 - If tax residency country is selected as USA, then under FATCA details section, user needs to capture in Other Details section like Is it a Financial Institution?, Type of Financial Institution, Party GIN, and so on.

-
- If tax residency country is selected as other than USA, then a new section called CRS section is enabled and it needs to be captured. This section contains fields like Is it a Financial Institution?, Type of Financial Institution, and so on.

6.6.6 Other Details

- The Other Details section captures detail of the party like whether the party is exempted from cash transactions, whether the party is related interest of the insider or not.
- CTR Details: A field to check whether CTR exemption is available, if this is selected, then the date of exemption field becomes mandatory.
- Insider Details: Supports modification and inquiry of insider details.
 - The details captured during onboarding are displayed.
 - User can also view, add, edit, or delete insider details.
 - A party can be related interest of an insider or not related. If the party is identified as a related interest of insider, then the fields to capture the insider details is enabled.

6.6.7 Consents

- The Consent section allows the banker to capture the following details about the party:
 - Consents
 - Anti-Money Laundering Characteristics
- The list of consent question values are factory shipped. Additionally, the bank adds its own list during parameterization. This list is different from the Individual party type's consent questions.
- Anti-Money laundering characteristics are captured from this section.

6.7 Profile: Trust

Party Profile widget stores general information about the party. Some of this information is captured at the time of onboarding itself, and is available for viewing and updating. In addition, the Profile widget makes additional fields available where more information about the party are maintained.

Unless otherwise stated, the functionality described below applies to all the roles such as Customer, Service Provider, and Affiliates.

The Profile widget displays the following details in the Summary page:

- Constitution
- Role
- Home Branch
- Customer Since
- Last Activity on
- Established on
- Industry

- Country of Establishment
- Relationship Manager

All the details in this page are read only. The user can use the Maximize button provided in right top end corner to navigate to the Profile child page, which allows to view and edit of profile information.

The Profile child page supports the following sections:

- General Information
- Identification
- Financials
- Blacklisting
- Legal Reporting
- Other Details
- Consents

The details of each section are explained in detail in subsequent sections below. All the existing functionalities will continue to exist unless specifically mentioned in this document.

- The General Information page stores information about the party. Some of the details captured during party onboarding are defaulted in this page and are available for view and modification.
- All the fields are pure data capture fields which are populated from the onboarding page or are captured here in Update mode and are available for modification.
- The General Information page is further divided into multiple sections as listed below:
 - Basic Details
 - Trust Details
 - Other Details
 - Role Details
 - Beneficiary Details
 - Direct Entry Identification Details
- Each section is discussed in detailed in the subsequent points.
- Header: The General Information section header displays the Party Name, Party ID, and General Information.
- Organization Details section:
 - The user captures the basic information related to the party entity such as the Constitution, Industry Code, Incorporation Country, and Place of the Trust.

Note

The Country of Registration is captured at the time of onboarding. Currently, there is no linkage between this field and the Country of Incorporation field.

- The Customer Segment is a drop-down field and contains the list of configured segment values that the user can select. This is an optional field.
- Trust Details section: This section captures the basic trust related details like Industry, Trust Establishment Date, Constitution and Country of Registration, and so on.
- Other Details section: This section displays the other miscellaneous details related to the party entity.
- Role Details section:
 - Same as for Individual party type.
 - Exception: For Broker and Introducer role type, the additional details captured for Organization is different from an Individual.
- Beneficiary Details section:
 - This section captures the list of beneficiaries of the trust. The beneficiary details captured during onboarding are defaulted here.
 - The beneficiary details are not mandatory and can be deleted. During onboarding however, the beneficiary details grid is mandatory.
 - Address of the beneficiary is captured here which is not captured during onboarding.
 - The contact number of the beneficiary is captured. This is an optional field.

6.8 Relationships

Oracle Banking Party Management supports mapping, maintenance, and management of inter-relationships between parties. The relationships are created as part of the day zero set up. When parties are onboarded or subsequently as part of the servicing functions, bank maps various parties to each other, identifying them with their relationships. These relationships between parties are then used in a variety of places within the Oracle Banking Party Management application, such as to enable access to accounts, share income, collaterals, and so on.

Broadly speaking, all relationships are classified into two Relationship Types within Oracle Banking Party Management that are, Personal and Business.

- Personal relationships are those which are personal in nature, such as those between family members, friends, and relatives. Some examples of personal relationships are father, mother, son, daughter, and so on.
- Business relationships are those which are of a non-personal in nature, such as directors (of a company), partners (of a firm), power of attorneys, authorized signatory, and so on. Business relationships are further divided into relationship class, based on the role played by that particular relationship for the party. There are three types of relationship classes:
 - Owner: Examples of relationship under this class are Promoter, Shareholder, Partner, Proprietor, and so on.
 - Administrator: Examples of relationship under this class are Authorized Signatory, Mandate Holder, Power of Attorney, and so on.
 - Other: This is the residual class that groups relationships other than Owners and Administrators. These could be Personal relationships such as father, mother, daughter, and so on or Business relationships such as group company, business associate, and so on.

The Relationships widget displays the following details in the Summary page:

- Parties (Number of party to party relationships maintained): Currently only number of direct relationships are shown here.
- Groups (Number of groups the party is a part)
- Borrowing Entities (Number of borrowing entities the party is a part)

All the details in this page are read only. The user can use the Maximize button provided in right top end corner of the page to navigate to the Relationships child page, which allows to view and edit the relationships information.

The Relationships child page supports the following sections:

- Party to Party relationships
- Groups
- Borrowing Entities

The details of each section are explained in subsequent sections below. All the existing functionalities continues to exist unless specifically mentioned in this document.

6.8.1 Party to Party Relationship

By default, this section is shown in Read mode with Update (create and update functionality are merged into update) and Print buttons enabled. On clicking Update button all the fields in this page alone becomes editable with the OK and Cancel buttons enabled (Update button are disabled, Print is always enabled).

In case of Update mode, the user cannot navigate from one section to any other section in the same page or move to any other page without clicking the OK or Cancel button.

- The Party to Party Relationship section captures and maintains the party to party relationships. It displays all the entities related to a party, including their privileges. It also allows adding or removing relationships to the party.
- The user can perform the following operations from here in Update mode:
 - Add New Relationship
 - Remove Existing Relationship
 - Edit Existing Relationship
 - Link New Affiliates to Account
 - Delete Existing Affiliate from an Account
 - Change Mandated Authority
- Relationships can be created between existing parties in the system or the related party can be onboarded.
- After creating a relationship, this section can be used to link the related party to the account of the main party. Continuing the above example, once relationship is created between A and C, the user can link to the accounts of A. This is known as party to account relationships (in the subsequent sections, this functionality is discussed in detail).

Process: Parent Party selection and Relationship selection

- On entering the party ID, the system displays the parent party details: Party ID, Full Name, Customer Type (Individual, Trust or an Organization), and Constitution (for non – individuals).

Note

While adding the related party, the difference between an organization, trust and individual is that for individuals, system displays the first name and last name and no constitution. Whereas for organization and trust, system displays the name and constitution.

- System checks if there is an existing party to party relationships for the party.
 - If relationship does not exist, then system displays the section for adding new relationship.
 - If relationships already exists, then system displays the existing relationships .
- In the Add Relationship section: Along with the parent party, the system also displays the relationship class and relationships .

Note

All the parties which are related to party are also displayed here and the party selected above is also displayed here.

- User selects the parent party and then the relationship class (Owner, Administrator, and Other). Based on the relationship class selected, the system displays the corresponding section:
 - New Administrator
 - Add Owner Details
 - Add Relationship Details
- When user selects the relationship name, the system checks whether there exists more than one inverse relation for the relationship.
 - If no, then system displays both the direct and indirect names.
 - If yes, then system displays the direct relationship name and makes the indirect relationship name as picklist and editable. Here, user has to select one of the indirect relationship names.

Example: If the user selects the direct relationship as Father, then system displays Son and Daughter in the inverse relationship name.

New Administrator - New / Existing Party

- System displays the details for adding new administrator parties. User can select Existing Party as No, to indicate that the party to be added is a new party, and enter the following details:
 - User enters the Name (first name and last name) and Email ID.

Note

Just the name and email is entered here, party is onboarded in the next step. For more information, refer section below.

- If an existing party exists, then we can directly search and select them.

- Party type is defaulted to Individual (as only individuals can be administrators).
- User can select the relationship name using the search provided. The relationship name list is fetched based on the parent party type, constitution, and relationship class selected above. Based on the relationship name selected, the system displays the relationship type (Personal or Business - as read only).
- Documents: User can also upload documents. For example, user wants to upload the power of attorney document against the relationship being added.
- If it is a new party, the system displays the page for party onboarding.

Add Owner

- In case user has selected the relationship class as Owner, the system displays the details for adding owner parties.
- The details or flow is same as adding an administrator. In addition to that, the system displays a field to capture percentage of ownership.
- The party type is selected by the user in case of new parties and defaulted to the searched party in case of existing parties.

Note

Onboarding a new party through this page is applicable for Add Owner also (like Add Administrator - New party).

Add Other Relationships

- In case the user has selected the relationship class as Others, the system displays the details for adding other relationships. The details or flow is same as adding an administrator.

Link Accounts

- As part of add or edit relationship, the user can link the accounts to the party also.
 - The system displays the account List in the section with option to link the party to the selected accounts.
 - Details displayed are Account Number, Account Holder, Account Type, and Account Title.
 - User can select one or more accounts for linking to link the accounts to the party.
 - The user to add mandated authority for the new affiliate. For each of the account, the system displays the list of related parties, each row having the details of Party Type, Relationship Class, Party Name, Relationship, and Mandated Authority.
 - System links the party to the accounts and displays it in the Relationship Summary page.
 - The Link Accounts section does not appear if the relationship class is Others.

Relationships Summary

- The user can add more relationships by clicking on Add Relationship button (in this case, the process of adding relationship continues and after entering the details the Summary page is displayed again with new relationship). The new relationship can be added for the newly created party also by selecting from the parent party picklist, that is the system displays the new party also in the parent

party picklist, once the party is successfully added.

- If a relationship is captured, then the system displays the Relationships Summary page. For each of the relationships, the system displays the options to,
 - View relationship details
 - Edit relationship
 - Delete relationships

6.8.2 Groups

- Group could be termed as a group of customers (or members) who are related or associated to each other or any of the members of the group.
- A customer can be part of many groups as the relation of a party with certain other parties differs.
 - There can be certain groups where a party is a part due to business reasons. For example: In one group as the party is the major distributor of goods for another party.
 - The same party can have personal relations and can be in another group due to the virtue of this personal relation.
- The decision on whether the party has to be considered for credit decisioning and for viewing exposure is decided at a submission level.
- Groups section is introduced in the Relationships widget. This is a read only page.
- In this section, the system displays all the groups in which the party is a part. The system displays the following group details:
 - Group Name
 - Group ID
 - Group Description
 - Party names of all the group members

6.8.3 Borrowing Entity

- Borrowing entities are created in LCM for the combination of applicants applying for the various product groups (belonging to asset and credit card).
- Borrowing entities section is introduced in the Relationships widget. This is a read only page.
- In this section, the system displays all the borrowing entities in which the party is a part. The system displays the following borrowing entity details:
 - Borrowing entity name (all party names in comma separated)
 - Borrowing entity ID
 - All the Facility IDs and Product Group names linked to this Borrowing entity.

Note

The details displayed in this page is pulled from an external module.

Hence, for Oracle Banking Party Management, the details are not displayed, but product hooks are provided to fetch the details from the module and display the same.

6.9 Holdings

- The Holdings widget displays the Assets, Liabilities, and Insurance maintained by the party with the bank.
- This widget is dynamically populated with the latest real time data.
- Only the accounts where the party is the primary or joint applicant are listed here.
- If the party does not have any account relationship, then a default message is displayed saying no holdings maintained with the bank.
- The Holdings widget displays the following details in the Summary page:
 - Header - Holdings
 - Assets (total number of accounts held) - Total amount of assets (converted in home branch currency)
 - Product Type (number of accounts held) - Total amount (converted in home branch currency)
 - and so on ..
 - Liabilities (total number of accounts held) - Total amount of liabilities (converted in home branch currency)
 - Product Type (number of accounts held) - Total amount (converted in home branch currency)
 - and so on ..
 - Insurance (total number of accounts held)
 - Product Type (number of accounts held)
 - and so on..
- The logic used to display the product types applicable to each of these section is listed below:
 - Assets: All product types such as Asset and Credit Card are displayed in this section.
 - Liabilities: All product types such as Liability, Investment are displayed in this section.
 - Insurance: All product types such as Insurance are displayed in this section.
- All the details in this page are read only. The user can use the Maximize button provided in right top end corner of the page to navigate to the Holdings child page, which allows to view all the holdings information in detail.
- Header: The General Information section header displays the Party Name, Party ID - Holdings.
- The Holdings widget child page displays the account holdings under the following sections:
 - Assets
 - Liabilities

-
- Insurance
 - Other Accounts
 - Each section is discussed in detailed in the subsequent points.
 - Assets section:
 - The Asset section displays the assets of the customer that is, deposit products like term deposit, savings and checking accounts. It also covers the investment accounts of the party.
 - The system displays the total assets amount maintained by the party with the bank across different asset accounts in home branch currency.
 - It also displays all the accounts maintained by the party with the following information:
 - Product Group name
 - Ownership pattern (sole or joint ownership)
 - Plan Code (for investment only)
 - Account number
 - Current account balance (in home branch currency)
 - Bundle name (if account is part of a bundle, else it is hidden)
 - Liabilities section:
 - The Liabilities section displays the liabilities of the customer that is, credit card and loan products like loans, overdrafts, and overdraft accounts.
 - The system displays the total liabilities amount maintained by the party with the bank across different liabilities accounts in home branch currency.
 - It also displays all the accounts maintained by the party with the following information:
 - Product group name
 - Ownership pattern (sole or joint ownership)
 - Account number (card number in case of credit card)
 - Current outstanding account balance (in home branch currency)
 - Facility description
 - Bundle name (if account is part of a bundle, else it is hidden)
 - Insurance section:
 - The Insurance section displays the insurance products owned by the customer that is, insurance policies.
 - It displays all the insurance products maintained by the party with the following information:
 - Product group name
 - Ownership pattern (sole or joint ownership)

- Policy number
- Premium (in home branch currency)
- Expiry Date
- Other Accounts section:
 - The Other Accounts section displays the other accounts of the customer that is, where party is a affiliate, co-signor, or owner.
 - It also displays all the accounts where the party to account relationship is as explained above with the following information:
 - Product group name
 - Relationship
 - Account number
- All the details in this page are read only.
- In all the 4 sections explained above, for each account there is a P2A icon which is a hyperlink, and if the user clicks this icon, the Party to Account Relationship page appears:

Note

For credit cards, investment plan, and insurance policy, the Party to Account linkage is not applicable. Hence, the P2A link is hidden for them.

The Party to Account Relationship page details are explained in detail in subsequent section.

Party to Account Relationship

- From the Holding page, on clicking the Party to Account (P2A) icon from any account, opens this page.
- This page displays all the parties linked to an account. The page is used to view, add, or remove parties to or from an account. The parties can be added as joint accounts or affiliates.
- By default, this page is displayed in Read mode with Update (create and update functionality are merged into update) and Print buttons enabled. On clicking the Update button, all the fields in this section alone becomes editable with OK and Cancel button enabled (Update button is disabled, Print is always enabled).

Note

In case of Update mode, the user cannot navigate from one section to any other section in the same page or move to any other page without clicking the OK or Cancel button.

- The below steps describes the functionality for party to account relationships:
 - The system displays the basic account details like Party Name, Outstanding Balance <Outstanding Balance>, and Show Details link (this link is a generic link displaying the account information).

- The page is divided into two following sections:
 - Account Party Relationship Details
 - Link Affiliates to Account

Account Party Relationship Details section:

- The following operations can be performed for the Account Party Relationship Details section:
 - Add Party to Account (new or existing party)
 - Change the relationship
 - Remove an existing party
- If the user clicks the Add Party to Account button, the system displays the section for addition of a new relationship. User is able to search for an existing party and add the relationship or add the relationship for a new party, which triggers onboarding of the party.

Note

User is able to add parties with non customer roles also as account holders.

- Change the relationship: User can open the Relationship (SOW/JAF/JAO) picklist and change the relationship as required. User can replace and add customer to the account relationship at one time.

For example: Suppose a customer has SOW relation and wants to add another customer as JAF, then first SOW relationship has to be changed to either JAF or JAO from the drop-down list in the section. After that, user can add another customer as JAF to the account (from Add Customer button). If the adding customer is to be JAO, then existing customer should be JAF.

Note

The change of applicants to asset accounts is not permitted from this page, but performed from Change of Borrower page. However, the party to account relationship service is made available for other modules to perform changes such as change of borrowers.

- Remove an existing party from an account: Click on the Delete icon to remove the required relationship.
- On successful change or deletion of relationships, the system does the following:
 - System logs the events for alert generation for added, modified and removed relationships .
 - System re-evaluates the risk indicators.
 - If a party is deleted from an account, the debit block rule is run again, and based on the result it restores the earlier status of the account.
- Party's relationship to an account (Individual type: Account in which primary party is of Individual party type) can be one of the following:

Table 6–2 Party Relationship: Individual type

Relationship	Relationship Code	Party
Sole Owner	SOW	Primary
Joint And First	JAF	Primary
Joint Or First	JAO	Secondary

- Party's relationship to an account (Trust type: Account in which primary party is of trust party type) can be one of the following:

Table 6–3 Party Relationship: Trust type

Relationship	Relationship Code	Party
Sole Owner	SOW	Primary

Link Affiliates to Account section:

- User can change the mandated authority for the affiliate linked to an account.

6.10 Risk Indicators

This page is displayed in Read mode with Update (create and update functionality are merged into update) and Print buttons enabled. On clicking the Update button, all the fields in this section alone becomes editable with OK and Cancel button enabled (Update button is disabled and Print button is always enabled).

In case of Update mode, the user cannot navigate from one section to any other section in the same page or move to any other page without clicking the OK or Cancel button.

The child page in Risk Indicator widget displays the following common link icons for easy navigation:

- Contact Details: Displays the preferred address and contact email information
- Memo Details: Displays the active memos
- Close: Back to the landing Single Party View page

The Risk Indicator widget displays the risk indicators maintained for the party. Only active risk indicators linked to the party are displayed. The summary page displays only upto three indicators, on a first come first serve basis.

To view the rest of the risk indicators the user needs to navigate to the child page.

If the party does not have any risk indicator, then a default message is displayed saying no risk indicators are maintained for the party.

All the details in this page are read only. The user can use the Maximize button provided in right top end corner of the page to navigate to the Risk Indicators child page, which allows to view and edit all the risk indicators.

- The Risk Indicator page is a new Re-UXed page. From the Manage Risk Indicators page, the user can view, create, or delete the risk indicators.

-
- The list of risk indicators is from seed data and bank can add more indicators if required during implementation.
 - The following seed data values alone will make the date field mandatory:
 - Deceased
 - Bankruptcy
 - Fraud
 - For all other risk indicators, the date field is disabled.
 - The system also supports capturing remarks, which is an optional field for all the risk indicators.
 - Once the indicators are captured using this page, these indicators are shared with other modules and sub-modules, so that they can process based on captured indicators.
 - Deletion of risk indicator can happen from this menu only.
 - Some system risk indicators are also available, which is placed and removed by the system, and the user can only manually view them and is not allowed to add, edit, or delete them.

6.11 Due Diligence

By default, this page is displayed in Read mode with Update (create and update functionality are merged into update) and Print buttons enabled. On clicking the Update button, all the fields in this section alone becomes editable with OK and Cancel button enabled (Update button is being disabled, and Print button is always enabled).

In case of Update mode, the user cannot navigate from one section to other section in the same page or move to any other page without clicking the OK or Cancel button.

The child page in Due Diligence widget displays the following common link icons for easy navigation:

- Contact Details – Displays the preferred address, contact email information
- Memo Details – Displays the active memos
- Close – Back to the landing Single Party View page.

The Due Diligence widget displays the current due diligence details maintained for the party. The summary page displays the status of the following:

- KYC
- AML
- Tax

To view more details about the due diligence status the user needs to navigate to the child page.

All the details in this page are Read only. The user can use the Maximize button provided in right top end corner to navigate to the Due Diligence child page, which allows to view and edit all the due diligence details.

- The Due Diligence child page is part of Due Diligence widget.
- The Due Diligence page displays the following:
 - The status of the due diligence check
 - The actions applicable against each due diligence check.

- The identity verification checks against the due diligence check.
- The statuses of the identity verification checks for each mode of verification (Electronic and Manual).
- The actions applicable against each identity verification.
- Actions applicable against each Due Diligence check are as follows:
 - If the status of the due diligence check is Pending or In progress of the action, View History is available against the due diligence check.
 - If the status of the due diligence check is Confirmed, Unconfirmed, Not Applicable and Cancelled, the actions View History and Reinitiate are available against the due diligence check
- Actions applicable against each identity verification check are as follows:
 - If the status of the identity verification is Confirmed, Unconfirmed, Not applicable and Cancelled then the action View is available against the identity verification checks.
 - If the status of the Identity verification is Pending , In progress then the actions View and Cancel is available against the identity verification.
 - If the status of manual verification is In Progress, then the action Verify is available against the manual verification
 - If the status of the electronic verification is Pending, then the action Initiate is available against the electronic verification.

6.12 Credit Worthiness

The Credit Worthiness includes the qualitative analysis of the credit assessment. It aims to provide the banker a set of information about the past performance and conduct of the existing accounts of the borrower which in turn gives input to the banker on the Character of the borrower. The borrower credit rating is also giving an input to the character of the borrower. By default, all the sections in the page is displayed in Read mode with Update (create and update functionality are merged into update) and Print buttons enabled. On clicking the Update button, all the fields in this section alone becomes editable with OK and Cancel button enabled (Update button is disabled but Print button is always enabled).

In case of Update mode, the user cannot navigate from one section to any other section in the same page or move to any other page without clicking the OK or Cancel button.

- The Credit worthiness widget displays the current information regarding the credit worthiness maintained for the party. The summary page displays the status of the Risk Scores/Metrics captured. If no risk score is captured, the widget displays message as No Risk score available.
- The summary displays the latest 3 entries in the following format:
 - Risk Type Description <Space> Score, Rating, Risk Grade (Effective date)
 - Metric Description <Space> Metric value (Effective date)
- To view more details about the Credit Worthiness the user needs to navigate to the child page.
- All the details in this page is Read only. The user can use the Maximize button provided in right top end corner to navigate to the Credit Worthiness child page, which allows to view and edit all the credit worthiness details.

-
- The Credit Worthiness child page supports the following sections:
 - Risk Scores
 - Breaches
 - Bureau Report
 - Credit Exposure
 - The details of each section are explained in detail in subsequent sections below.

6.12.1 Risk Score

- In this section, different types of credit metrics and risk scores for a party are maintained. These metrics and scores are typically expected to be generated by an external system and updated into OBP through an interface. However, the section also supports manual capture and update of these parameters.
- These parameters are used by the bank as inputs in the credit assessment process.
- User can capture various types of credit scores and metrics for a party.
 - Credit scores of parties of all party types and roles and can be captured, though the usage is expected for customers only.
 - The credit scores are maintained at enterprise level.
 - The user can perform the following types of operations:
 - View an existing record
 - Create a new record
 - Update an existing record
 - Delete a record. Deletion is performed for individual line items within the grid and not for the party record as a whole.
- Records with Effective Date older than 7 years are purged through a batch process.
- Credit Details:
 - All the fields are displayed only in fields. Records entered in the grid below are displayed.
 - The records in the grid are sorted Effective date wise that is, latest (last) Effective Date first and within it, first risk score and then metric type
- Classification:
 - The user chooses the type of record to add or modify that is, risk score or metric.
 - Selecting one of the two is mandatory.
- Credit Metric:
 - Metric Type: Values of the drop down (Credit Risk Rating and Probability of Default) are factory shipped and can be added by the bank during day Zero configuration.
 - Effective Date: Can be a current or a future date but not a past date.
 - A combination of Party – Metric – Metric Type – Effective Date constitutes a unique record and if the user tries to create another record, system displays an error message and does not allow to save. However, a record with a different effective date can be created.

- Risk Score:
 - Score Type: The values in the drop down are a closed enumeration and cannot be changed.
 - Effective Date: Can be a current or a future date but not a past date. Defaulted as the current system date. A combination of Party – Risk Score – Score Type – Effective Date is a unique combination and if the user tries to create another record, system displays an error message and does not allow to save. However, a record with a different effective date can be created.
 - Other Risk Score Type: The values in the drop down are factory shipped and can be added by the bank during Day Zero configuration
 - Score: This field indicates the actual risk score of the party. It should be a positive integer, decimals are not allowed.
 - Rating: This field indicates the rating of the party. It is a text field.
 - Agency: This will be a LOV field (Configured as part of Day Zero using OPA006 menu) and displayed in the Manage Scores Table.
 - Rating Status: It stores the rating status as captured in the external system. Special characters are not allowed.
 - Rating Model: Indicates the model which is used to determine the score. Special characters are not allowed.
 - Risk Grade: This is used to store the risk grade associated with the risk score.
 - Scorecard Index: This field is used for referencing the scorecard index from the external system. It indicates a positive number, decimals are not allowed.
 - Scorecard External Reference number: This field indicates the reference number of the record in the external system from where it is being sourced.
- In case of Customer Merge, the records related to Credit Assessment of both the parties are retained under the party ID of Survivor. If records for Party ID – Metric / Score – Type – Effective Date match exactly (which needs to be a unique record), the records for the survivor are retained.

6.12.2 Breaches

- Breaches: This section displays details of any conditions and covenants for a party which is in overdue status across facilities. Conditions and covenants are displayed in two separate expandable or collapsible sub-panels.
- Conditions Breached – number of conditions breached is calculated by Origination and displayed in the header in brackets.
- Covenants Breached - number of covenants breached is displayed in the header in brackets.
- There is no change to the functionality of this section.

Note

The details displayed in this page are pulled from an external module. Hence for standalone party the details are not displayed, but product hooks are provided to fetch the details from the module and display the same.

6.12.3 Bureau Report

- Bureau Report tab provides an ad hoc menu option to fetch existing reports or initiate a new bureau call with the Credit or Debit bureau.
- This page can be used for party with any role in the system such as a Customer, Guarantor or Affiliate, except a Member.
- This page can be used for all three party types like Individual, Trust and Organization.
- Since this is not a servicing page, the memo related to the party is not displayed.

6.13 Credit Exposure

- The Credit Exposure page displays the party level exposure only. Exposure details are displayed across Business Units (BU) or LOBs (Line of Business). This is a read only page.
- The user can view by Exposure value or LVR %. Also under Exposure value, the details are further broken into:
 - Direct exposure
 - Guaranteed exposure
 - Related exposure
- Click on the link to generate the report , LCM considers the proposed facility, charges, and collaterals including the current in-flight submissions to generate the file summary report for the party.

Note

The details displayed in this page are pulled from an external module. Hence for standalone party the details are not displayed, but product hooks are provided to fetch the details from the module and display the same.

6.14 Notifications

- This widget contains all the current updates of pending events related to the party.
- Click on the Expand icon, Notifications child page displays all the notifications with vertical scroll if required. This is a read only page and does not have any link to different pages.
- If no notifications exist for a party then in this widget message is displayed as No Notifications exist
- These notifications is displayed from the time the event is triggered till event is closed or resolved.
- The Notifications is not displayed in any particular order. If the length of the Notifications is more than 1 line, then it is shortened with ... and on mouse hover user can view the full contents. Also, if only 1 notifications is available then it displays the entire content if more than 1 then it displays ...
- There is a maximize button available at the right bottom end of this widget which opens the Notifications child page to display all the Notifications entries, if more than 3 entries are available in the page.

6.15 Calendar

- The Calendar panel is a new Panel drawer item in Single Party View page.
- This panel displays the calendar with options to view them by Day, Week, Month and List. The events that are expected on a particular date is displayed. In case of more entries in a day - on selecting the More Link, the system displays all the Events information.
- The list of events currently supported by the calendar widget are:
 - KYC Expiry date
 - Loan repayment dates (Title: Loan Account < Account Number>, Description: Installment Amount <CCY Code Amount>)
 - TD Maturity dates (Title: Term Deposit <Account Number>, Description: Maturity Amount <CCY Code Amount>)
- In future, more events can be added as the infrastructure is available from now on.
- These events shown in the calendar appears from the time the event is triggered or identified or created for both past and future time period of 1 year or data is purged from the database. Hence, user can view the past and future date events and also Inbound and Outbound documents.

6.16 Documents

The Inbound documents panel is a Panel drawer in Single Party View page. This panel displays all the inbound documents of the Party classified into following:

- All Elapsed documents are displayed with Document name and Valid Till date so that fresh copies of these documents can be again received from customer and re-uploaded.
- All the Uploaded and Received but not Uploaded documents are also displayed. In case valid till is not maintained, then it displays as blank.

This is an existing Document Task flow page shown in CNM06 which is filtered to show only the following:

- Party – Context Party
- Document category - Outbound
- Status – All
- Document Type - All

The user can view, generate, dispatch, accept, execute or re-dispatch these documents.

7 Broker and Introducer Status Modification

This page allows the user to change the status of the Broker or Introducer.

The functionality for this page is as follows. Unless specifically mentioned, the rules given below apply to both Broker and Introducer roles:

- This page allows the user to perform the following:
 - Display and Update the status
 - Maintain the reason for change of status, if any
 - Status for the two roles is separately maintained that is, it could be Active for Broker and Inactive for Introducer and so on.
- In the Party ID field, only Party IDs with roles as Broker or Introducer are accepted. If the party ID entered has any other role, user gets an error message.
- The LOV for the Reason codes is derived from Common Services
- All status changes are updated to OCH immediately
- Not all status changes are possible from this page. The following table shows the possible status changes that can be done from this page:

Thus, it can be noted that:

- This page cannot be used to change the status of the service provider from anything to Deceased.
- This page cannot be used to change the status of the service provider from Terminated to anything else.
- The only changes possible are from Active to Inactive or Terminated and Inactive to Active or Terminated.
- Deceased: With respect to the status Deceased, the following is applicable:
 - Change of status to Deceased happens only automatically through system. This happens when user selects Deceased as warning indicator in the Party General Information (PI034) page.
 - Once the status is changed to Deceased, it cannot be changed back to any other.
 - The status Deceased is not applicable to Corporate Brokers.
- If KYC is required for the role, and is pending, system does not allow the status of the party to be marked as Active. First KYC needs to be confirmed and only then the status can be modified from this page as Active.
- The impact of status is that only service providers with status as Active appears in various LOVs.
- Commission Payments: The functionality of broker or service provider commission envisages payment of commission from an external OIC system. Oracle Banking Party Management only hands-off transaction data to OIC. For such hand-off, Oracle Banking Party Management will not filter out brokers or introducers based on status. The decision to pay or not to pay is left to the external system.
- Individual Broker or Introducer: In the case of Individual brokers, the status is maintained for a Business group and it is not per Broker. Hence, the page for Individual is slightly different with the

status summary displayed, and with edit and view links along with it. On clicking Edit, the status details are enabled for making any changes.

8 Associated Party

This page allows Associated Parties to be linked to an Account or to a Party. Associated Parties are akin to other relationships created in the system, but requires minimum details to be captured for linking. The current associated party types that are supported are:

- Solicitor
- Referee
- Nominee

The functionality of the page is given below:

- Associated Parties are always linked to one or more accounts. They require minimum details to be captured in the system, unlike Affiliates who need to be on boarded. KYC and deduplication checks are not applicable to associated parties.
- This page allows user to create associated parties and linking them to one or more accounts, or delinking the linked associated parties from the accounts.
- For Associated Parties, system generates a Party ID and assigns the role of Associated Party.
- The Associate Party ID – Account Number – Relationship forms a unique combination within the system.
- Currently, system supports the following to be linked as Associated Parties:
 - Nominee
 - Referee – Associate or Friend
 - Referee – Relative
 - Solicitor
- In this page, user is prompted to choose between Link Associated Party to Party and Account. If party is chosen, system displays all the accounts belonging to the party, wherein the party is an Applicant (SOW /JAF/JAO) or an Affiliate. User can select one or all the accounts and add associated parties. Thus, associated party is an account level association only.
- Account Details: If party is chosen in the previous field, the account details displays all the accounts belonging to the party. User can select one or more accounts to add the associated party and on clicking the Add Associated Party button, the next accordion invokes.
- Party Info: User decides whether the party is an existing party with the bank or not.
 - Yes: If the party is an existing party with the bank, system invokes the Common Party panel where user can input the Party ID of the party. This displays the Party details and allows the user to link the Relationship (Nominee, Referee, so on...) and proceed.
 - No: If the party is not an existing party with the bank, user is prompted to select whether the party is an existing Associated Party with the bank.
 - Yes: If user selects Yes, system invokes the Associated Party Search pick list which displays all the existing Associated Parties in the system.

User can select a record from this list and click OK. System displays the selected party's details and allows the user to proceed.

- No: If the user selects No, system invokes the Associated Party Details accordion, where the user can capture the relationship as well as the personal details of the party.
- Associate Party Details: For an existing party or a new party to be added, this accordion displays and captures the party details and the associate relationship that the user can link to.
 - Associate Relationship drop down displays the four relationships as mentioned above.
 - Associated Party Type displays and captures the applicable party type. Based on the selection, the other fields get orchestrated for capture or display the party details such as name, date of birth and so on..
 - Subscriber ID generated in PEXA is fetched and displayed as part of associated party details. Once the user captures and saves the party details .The Subscriber ID for the party can be viewed in Read mode and Update mode as a display only field.
- Fetch Checklist: This action button allows the user to upload documents, if any applicable to the linkage. The documents need to be configured in the Inbound Documentation module, which allows relationship wise documents to be maintained (Refer page CNM03 Document Policy Definition). All the maintained documents is displayed in the pick list and user can identify the document and upload.
- Relationship Specific Details: This accordion is enabled only if the relationship chosen is Nominee. It captures the following two details of the nominee:
 - Percentage share of the nominee
 - Relationship with account holder
- Add Nominee: For relationship Nominee, it is possible to add multiple nominees by clicking on the Add Nominee button which performs an intermediate Save and allow the user to add another nominee.
- User can also delink an existing linkage by invoking the page in Update mode, selecting a record and clicking on the Delink. System does not perform any validations and delinks the record immediately.
- Delink means only removing the Associated Party – Account linkage. The party continues to remain in the system.

9 Enquiry and Party Search

9.1 Basic Search

Party Search is an important functionality in the party module. Two types of searches are supported in the module that is, Basic search and Advanced search. Basic Search allows the user to search for party details based on some selected criteria such as Party name or Party ID. The advanced search is a common task flow which invokes from various places in the application, wherever there is a need to search for a party. Party Search panel also appears as a panel on the left side of the Oracle Banking Party Management page, so that user can search for a party at any point of time.

- Using the Basic Search panel, user can search for parties.
- User first needs to select the criteria for search from the dropdown Search By.
- The four parameters available are: Name, Account Number, Party ID, Email ID and External System ID.
- Then, user can input the value for search criteria in the input field provided:

The details on how each search criteria works is briefed below:

- Name:
 - The search for name is based on First Name in case of individuals and Legal Name in case of trusts and organization.
 - The search is not an exact search, user can enter only the first few characters and click on the Search, system displays all the matching results in a list from which user can select the preferred match.
 - Search cannot be conducted with a string which does not include the starting characters. Please see the examples below:

Party Name	Search String	Result
John Smith	John	Success
John Smith	Smith	Full Name was not found
John Smith	Joh	Success
John Smith	Smi	Full Name was not found
National Carriers	National	Success
National Carriers	Carriers	Full Name was not found

Party Name	Search String	Result
National Carriers	Nat	Success
National Carriers	Carr	Full Name was not found

- Note that when more than one result satisfies the search, all the results are displayed. For example, in the above example, if search is conducted on Joh (case 3), system retrieves all the parties with first names starting with Joh such as John, Johanna, Johnny and so on.
 - If no record matches the search criterion entered by the user, system displays the message as "Full Name not found."
- Account Number:
 - User can input the account number and perform the search.
 - The full account number can be entered. This is an exact match. If only a part of the account number is entered, system displays the message as "The account was not found."
 - If the account has joint holders, names and party IDs of all the joint holders is displayed in a drop down. User can select the holder's profile to view.
 - Party ID:
 - User can input the party ID and perform the search.
 - The full party ID should be entered. This is an exact match. If only a part of the party ID is entered, system display the message as " The party ID was not found."
 - The ID could pertain to a customer or a party in any other role such as an affiliate or a service provider.
 - Email ID:
 - User can input the email ID and perform the search.
 - The full email ID should be entered. This is an exact match. If only a part of the email ID is entered, system display message as "The party ID was not found."
 - Email ID search is not applicable to trusts and organizations.
 - External System ID or CGID:
 - User can input the External System ID or CGID and perform the search.
 - The full external system ID should be entered. This is an exact match. If only a part was entered the system displays an error as "The External System ID was not found."
 - The search using external system ID happens in OCH and the results are fetched and displayed.

Search Output: When basic search query is successfully executed, system retrieves all the records which match the search string input by the user. If there are more than one record, system displays the list of all the party IDs and party names which match the query.

9.2 Advanced Search

- Advanced Search is actually a common task flow that gets invoked from various places in the application, wherever there is a need to search for a party. From the party context widget, on clicking the Advanced Search link, Advanced Search Panel displays.
- System invokes the party search wherein the user can choose the search based on Role or Party Type. The same page is invoked from various other places in the application, wherever party search is required to be conducted.
- If the user chooses Party Type, system invokes the Search By/Party Type panel wherein the user can input the desired party type or search an exact match.
- Based on the input entered by the user, system invokes a panel where the user can input the details such as party ID, name and so on... of the party by which user can conduct the search.
- If the search is required to be conducted based on Role, user inputs the desired role in the drop down and then captures the party type, name, IDs, and so on... or any other details based on which the search is required to be conducted.
- In case the Role is Broker or Introducer, additional fields are available by which the search can be conducted.
- Once the user inputs the desired parameters and click on the Search, system displays the search results in the Party Search Results panel. User can select a row and click Set Context to complete the selection and return to the main page.
- When more than one fields is entered for performing search, system uses the AND logic to perform search. For example, if first name is entered as John and last name is entered as Smith, all the individuals with names as John Smith will be retrieved, but John Howard or Ian Smith will not be retrieved.
- Search for Zip code is conducted under Address Type Home for individuals and Registered under organization and trusts. Search is conducted on Current Address and not on Future Address.

10 Data Privacy and Security

As part of the Global data protection regulation the following capabilities are supported in the system:

Purging

- Capability to purge some PII data elements of a party across Oracle Banking Party Management, that is party's PII details or documents needs to be deleted upon customer request (As long as it does not affect any other regulation, bank process or Oracle Banking Party Management system processing).
- Capability to delete data in such a way that data can no longer be re-created, accessed, or read using all reasonably available means.

Masking

- Capability to display only a portion of a data field or temporarily prevent viewing a data element.
- Capability to select from a list of PII data elements which needs to be masked as part of day 0.
- Capability to mask, tokenize, and hook for supporting tokenization is supported in Party onboarding (standalone, P2A and P2P) and Servicing pages.
- Capability to mask PII details in read only mode on the page (not in edit or add).
- Capability to mask PII details in read only mode (not in edit or add).

Tokenization

- Capability to enable or disable tokenization of PII data elements as part of day 0.
- Capability to mask, tokenize, and hook for supporting tokenization is supported in Party onboarding (standalone, P2A and P2P) and Servicing page.
- Capability to provide hook to support interfacing with third party tokenization system to retrieve the token and actual values.
- Capability to tokenize the specific PII details.

Customer Consent for Data Collection

- Configuration to enable or disable upfront consent capture from customer for data capture.
- Capability to capture the consent at the beginning of the data capture cycle and validations to stop data capture till consent capture.
- Capability to capture the consent at the beginning of the data capture cycle and validations to stop data capture till consent capture.
- Configuration to switch off the default consent functionality for all the existing and new party consents captured across onboarding and servicing page.

11 Core Components

This chapter describes the core components of Oracle Banking Party Management. These components include functionalities that are used to perform primary operations and to define the broad parameters within which the application functions.

11.1 Core Entity Services

Core Services enable the bank to configure the broad parameters such as bank and branch configurations that include defining the structure of the bank through maintenance of regional offices, lines of business and various branches, along with unique identification codes, financial cycles and accounting periods, followed by the bank, the policies of the bank, geographical locations (countries, regions, states, cities, and so on), languages and the different time zones in which the bank operates.

Following are the maintenance pages that enable the bank to configure various core entity parameters required for the bank to support its day-to-day primary operations.

- **Bank Codes (Fast Path: CS01):** This page helps the bank to define a unique bank code for the own bank.
- **Business Group (Fast Path: CS02):** This page allows the banks to define a group various product groups based on their line of business. This will help the bank accredit a broker or introducer to handle the offers that are part of a business group.
- **Bank Parameters (Fast Path: CS03):** This page allows the bank to configure various parameters such as bank name, address, bank currency, holidays, and so on.
- **Branch Parameters (Fast Path: CS06):** This page allows the user to configure various parameters such as branch name, address, branch currency, SWIFT and other payment network codes, and so on.
- **Country Codes (Fast Path: CS09):** This page allows the bank to configure countries and its time zones.
- **Reason Codes (Fast Path: CS16):** This page allows the user to configure multiple primary and secondary reason codes that the bank may want to stamp to a business event at different stages of the business process.
- **State Codes (Fast Path: CS17):** This page allows the bank to configure the states, province or emirates of a country.
- **Bank Policy (Fast Path: CS26):** Through this page the user can configure various policies of the bank related to AML reporting, unclaimed processing and so on.

11.1.1 Calendar Services

Calendar Services enable the bank to configure rule-based calendars for the different branches of the bank, currencies and payment networks that the bank deals with. It also allows the bank to define ad hoc holidays to handle unexpected situations that may arise due to natural calamity or government directive. The generic rule-based calendar configuration can be extended for a period of N years using custom scripts.

The Calendar functionality is achieved through the following pages:

- **Holiday Rule Maintenance (Fast Path: CAL01):** This page allows the bank to define the generic rules that need to be evaluated to mark a day as a holiday in a calendar. This rule is applicable for every calendar year defined.
- **Calendar Type Maintenance (Fast Path: CAL02):** This page allows the bank to define a calendar type and link the holiday rules. They can later attach the defined calendar type to a branch, currency or payment calendar.
- **Ad hoc Calendar Maintenance (Fast Path: CAL03):** This page allows the bank to define any ad hoc holidays to handle unexpected situations that may arise due to natural calamity or government directive.

The calendar services serve to record and retrieve the various holidays of the bank in a calendar year. Some of the most important services of this module that other modules use are as follows:

- Current working date
- Previous working date
- Next working date
- Working day check for a given date

11.1.2 Currency Services

Currency Services enable the bank to configure international currency codes, currency pairs, exchange rate types, buy and sell spreads, exchange rates, exchange rate history and attributes of various currencies such as spot days, decimals allowed or rounding, which can be used for various purposes by different products under Oracle Banking suite.

The Currency support functionality is achieved through the following pages:

- **Currency Codes (Fast Path: CY01):** This page helps the bank to configure the unique ISO currencies used in banking and business globally. This page also allows the bank to configure various currency related attributes such as adopted countries, spot days, decimals allowed, amount format and rounding rules.

11.1.3 Address Taskflow

Common Services also provides a generic address taskflow to configure any type of addresses such as home address, correspondence address, office address, collateral address, employment address, company registered address, branch address and so on.

The address taskflow is invoked wherever required and capture appropriate addresses. The address taskflow provides an option to the bank to capture a detailed address manually or using an integrated address search engine in a single line.

11.1.4 Questionnaire Framework

The Questionnaire framework enables the bank to define various questions that the bank may want to ask its customers during business processes such as determining offer eligibility during the application form capture process, loan account configuration, verification process, and so on. The answers recorded can be used for making various decisions or offer a product or service to customers.

The Questionnaire functionality is achieved through the following pages:

- **Section Maintenance (Fast Path: CS104):** This page allows the bank to configure various questions that they may want to ask during a business process to service the customer with appropriate products and services. This page also allows the bank to create conditions and dependencies to display the questions in a specific order.
- **Questionnaire Maintenance (Fast Path: CS103):** This page allows the bank to link the questions to the specific business process such as insurance application, offer eligibility check, loan account configuration, verification process, and so on.
- **Questionnaire resolution:** Questionnaire IDs can be configured for other modules as appropriate to the relevant business event where the questions need to be displayed for capturing the responses. During the specific business event, the relevant module makes a call to common services with the configured questionnaire ID to get the questions for capturing the responses. The captured responses are stored with unique instance IDs so that the responses can be edited at a later stage.

11.2 Multi Entity Multi Branding

The application provides a framework that enables enterprises to cater to their Multi Entity Multi Branding (MEMB) requirements using a single implementation of the application. The banking companies can make use of the MEMB framework to save costs in IT infrastructure and achieve operational efficiency.

Banking groups prefer to market several products under various brand names so as to get increased shelf space in the banking market. The different products they market are managed by several lines of businesses which act as independent units.

The solution provides flexibility for the banks to define multiple levels of entities as per hierarchy with in an enterprise. Users are always linked to the lowest level in the hierarchy. It gives the flexibility to resolve data for any entity above this level. Bank servicing units or branches can be configured to service one or more business units.

Users are mapped to a Home Business Unit and can have access to one or multiple Business Units.

Quite often it so happens that the products launched by the banking group under one brand compete with the products launched by the same banking group under some other brand in the market. In such cases confidential data should not be shared across the competing units.

Similarly, some Business Units in the enterprise offers products and services which complement each other. The data of such complementary units should be visible across the business units to reap the benefits of cross selling of products and services.

In order to reduce the overall investments in IT infrastructure, banking groups prefer to use the same IT infrastructure to cater to its entire banking empire of the enterprise.

The following key features of MEMB helps in resolving the data availability issues:

- Supports the co-existence of multiple entities within a single enterprise, such as Legal Entities, Market Entities and Business Units, while ensuring that system data is precisely partitioned between these entities.
- Facilitate information sharing across complementary business units.
- Ensure that confidential data is not accessible across competing business units.
- Robust and responsive to changes in information security policies over time.

The solution offers partitioning of data amongst multiple entities based on visibility rules configured for different categories of users of the bank and self-service channels for efficiently sharing and securing critical information across complementary and competing business units respectively.

11.3 Alerts

The following features are offered as part of Alerts.

- Alerts and bank notifications can be generated and sent to customers, cosigners, broker or introducer (only bank notifications), and some external parties for pre-defined events. The events can be financial and non-financial. On occurrence of such activity or events customers get alerts. Message templates can be maintained for each alert. The message template will be resolved based on a rule set up, in addition to the existing parameters.
- Dispatch of alerts can be deferred if alert dispatch type is selected as Deferred for Subscription type of alerts. In such cases, the alerts are not sent on occurrence of an event, instead they are put on hold and sent at end of day.
- Alerts can be dispatched to recipients such as, initiator of transaction on completion of approval process or to a broker on certain events occurring either due to the milestone being reached in Origination workflow or servicing events based off maintenance or transactions performed from Origination. For example: Account opening is an activity and CASA account opening can be an event under this activity. Fund transfer can be an activity which will have fund transfer credit event and fund transfer debit event.
- Rules can be defined for alerts based on business requirement. For example: Transaction amount greater than USD 100.
- Customers and some external parties of bank can also subscribe for specific events. The subscription for alerts can be for specific customer account.
- Alerts can also be sent to third parties such as brokers and so on.
- Alerts can also be sent to other related parties linked to the account apart from the account holders.
- Alerts can also be sent to Secure Mailbox.
- The alert template rule can be used to include a fixed outcome, if alert can be dispatched. This attribute can be used to handle scenarios where the bank may not want to dispatch alerts directly to customers when they have contacted the bank through a broker. The bank may want the notifications to be sent directly to the brokers who in turn manage the communications with the customer. This parameter brings the flexibility where bank can choose to notify customers or not depending upon the business model adopted by the bank.
- Alerts can also be sent from different email IDs and phone numbers, when alerts are to be sent by different market entities or business units.
- Other delivery channels such as mobile, app, or twitter can be configured, so that alerts hand off can be sent to those channels.

The above functionality is addressed in the following pages:

- Message Template (Fast Path: AL03)
- Alert Maintenance (Fast Path: AL04)
- Alert Subscription (Fast Path: AL05)

In cases, where the alerts have missed the desired recipient due to technical/DND or other reasons, alerts can be inquired and resent manually. This functionality is addressed in the Alert Support (Fast Path: AL10) page.

11.4 Content (Document Management System)

Documents form an integral part of any bank without which they are not able to perform their day-to-day business activities. Content offers the capabilities to manage documents and content. It is designed to provide a uniform set of services for content management across different modules. It serves as a standalone system for managing all the document related processes in an organization. These documents are basically of two kinds:

- **Inbound Documents:** Documents collected from customers
- **Outbound Documents:** Documents generated and dispatched to customers

These documents once defined can then be easily attached to individual processes or entities by creating some custom rules based on various parameters.

The following features are offered as part of Content.

11.4.1 Document Type Definition

A definition of every document to be used, whether inbound or outbound, can be created. Once defined a unique document type is created. Information like whether an inbound document type is recurring in nature or permissible delivery channels for an outbound document type can be captured here. Additional data like tags for inbound and inserts (scanned copies of additional materials to be sent along with documents) for outbound documents can also be specified.

A number of inbound document types can be logically grouped to create a document category. Documents under a category can be marked as mandatory or optional.

An inbound document that is received and stored in IPM can be retrieved and sent as an outbound document, like a covering letter, along with this particular inbound document as an insert.

The above functionality is addressed in Document Type Definition (Fast Path: CNM01) page.

11.4.2 Document Policy

Various rules can be created to help associate a document type or document category with certain processes or events or certain entities like party. Document Policy is assessed in runtime to determine what set of documents need to be collected or dispatched to respective bank customers. Policies can be created at Application, Collateral, Party, Product Group, and Submission level.

The above functionality is addressed in Document Policy Definition (Fast Path: CNM03) page.

11.4.3 Interface with Third Party Systems

For generation and dispatch of outbound documents, the capability is present to interface with multiple external third party document management systems. Various document templates stored in these systems can be accessed from Content module. The framework enables triggering of different API pertaining to different document generation systems. The document upload service can be consumed by other external system for enabling inbound document upload. The data sufficiency required to interface with external systems of physical documents storage is present. Additionally, services can be exposed for upload of documents that have been rescanned.

11.4.4 Document Checklists

Document Checklist is a taskflow that can be invoked by various modules at appropriate stages of a business process to view and act on both inbound and outbound documentation requirement that gets resolved as per

the document policy defined for a particular event or process. There is provision to upload inbound documents and create instructions for generation and dispatch of outbound documents from checklists. Various delivery channels like Post and Email can be specified for a document to be dispatched to a recipient.

Ability is provided to override the mode of delivery for one or all of the list of documents generated in the outbound checklist.

11.4.5 Regeneration and Resending of Documents

A configuration is available at service level to allow or suppress multiple regeneration of outbound documents in all tasks supporting outbound documents panel.

An inbound document given by a customer and stored in IPM can be retrieved and sent back to either the same party or customer, or to another email ID or mailing address as entered in the page or task flow.

11.4.6 Acceptance and Execution of Documents

For outbound document types, it can be specified whether they require customer acceptance and/or execution process. Any business process which generates this document type can use these flags and built a mechanism to track the acceptance of the document by the customer or execution of the document.

A separate taskflow is present for displaying documents which require acceptance or execution. User can manually update the status of documents once customer has accepted the document or a document execution has been completed.

11.4.7 Document Search and Upload

Soft copies of every inbound and outbound document are stored in an external system called Image Processing System (IPM) where versions of uploaded documents are also maintained. User can assess these soft copies anytime from Content module. Every uploaded document is given a unique index which helps in further processing of document.

Inbound document can be scanned for virus and malware before uploading in Documaker.

A separate page is provided for searching a document based on various parameters like document type, document status, indexes, and so on. The page can also be used for updating indexes, status and tags of a document.

The above functionality is addressed in Document Search and Upload (Fast Path: CNM06) page.

Documents which are not part of document policy can be collected from customer by uploading them from a separate ad hoc document upload page.

Upload of multiple documents is supported in application tracker and in verification task inside the inbound checklist page. The allowed limit for a single document file in multiple documents is 20MB and the total upload limit for all documents is 40MB.

Documents are allowed to be configured with expiry tracking types for inbound document after they are uploaded depending upon the document upload date, issue date of document or expiry date of document.

Both functionalities of questions related to the documents upload in context of verification and document for a set of questions is supported.

11.4.8 Document Upload by External System

System allows upload of documents for inbound as well as outbound documents and stores details of external system reference ID, external system name, receiver name and brand name with document type.

11.4.9 Services to Support Digital Channel

- Service to fetch deleted items for a digital channel.
- Service to accept digital acceptance for a digital channel.
- Ability to display the document type or document category differently in digital channel.

11.4.10 Stitching of Documents

Documents (external or uploaded or generated any of the types) can be inserted at the beginning or at the end of another generated document, such that all of them are stitched together as insert in one document through Documaker.

11.5 Rule Author

The Rules framework enables the bank to define various business rules, which are in turn used for specific purposes. It is a generic setup and used as a common module to define and resolve the defined rules.

Two flavors of rules can be defined - Decision Table and Guided Rule Editor. Facts are evaluated and used for defining inputs and the defined outcomes are given to the calling modules.

There are basic validations that the rule should be meaningful and complete. That is, the values of facts should be defined such that the evaluation will not remain incomplete. The number of facts and outcomes can also be defined by the business users. Maximum of 8 facts can be used to define rules.

Each defined rule belongs to a domain category and hence can be linked for the specific purpose of that domain category. The rules are attached at the respective placeholders in modules and executed at relevant places. For example, rules for asset classification, fees, interest setup, alert template resolution, and so on.

The above functionality is achieved through the following pages:

- **Rule Author (Fast Path: RL001):** This page helps the user to define a Decision Table and Guided Rule Editor based rule for a domain category.
- **Rule Simulator (Fast Path: RL002):** This page helps the user to evaluate the functionality of the defined rules by simulating a required scenario with sample test inputs.
- **Rule Search (Fast Path: RL003):** This page helps the user to search and view a defined rule.
- **Expression Builder (Fast Path: RL004):** This page helps the user to define various complex arithmetic expressions or formulas using facts and numerals. These expressions can be used while authoring a rule.
- **Filter Definition (Fast Path: RL005):** This page helps the user to define various filters that can be applied dynamically to identify certain details. The filters defined currently are being used to identify various accounts that qualify for collections. This functionality is specifically used in Collections module.
- **RuleSet (Fast Path: RULE01):** A RuleSet can be created using this page by grouping one or more rules that uses the same set of inputs. This functionality also helps to order the execution sequence of the rules where multiple rules need to be asserted for the same set of inputs. This functionality is specifically used in Collections module.
- **Rule Execution:** Rule IDs can be configured by other modules as appropriate to the relevant business event where the rule needs to be resolved. The modules call the rule resolution services at appropriate business events to evaluate the conditions to get the defined outcome.

11.6 Security Management System (SMS)

The application, comprising of several modules, has to interface with various systems in an enterprise to transfer or share data, which is generated during business activity that takes place during teller operations or processing. While managing the transactions that are within application's domain, it also needs to consider security and identity management and the uniform way in which these services need to be consumed by all applications in the enterprise. This is possible, if these capabilities can be externalized from the application itself and are implemented within products that are specialized to handle such services. Examples of these services include authentication against an enterprise identity-store, creating permissions and role based authorization model that controls access to not only the components of the application, but also the data that is visible to the user based on fine-grained entitlements.

11.6.1 Security

The application uses the best of breed components from Oracle's Fusion Middleware to deliver cutting edge solution in terms of a banking platform. The participating systems are as follows:

- Oracle Identity Manager (OIM) is used for managing user provisioning.
- Oracle Access Manager (OAM) is used for managing declarative authentication and SSO.
- Oracle Platform Security Services (OPSS) is used for runtime evaluation of authentication/authorization.
- Oracle Adaptive Access Manager (OAAM)/Oracle Adaptive Risk Manager (OARM) is used for step-up authentication and fraud management.
- Oracle Internet Directory (OID) is used as the identity/policy store.

For configuration details of the mentioned applications, visit the Oracle® Collaboration Suite Security Guide at http://docs.oracle.com/cd/B25553_01/collab.1012/b25494/toc.htm.

11.6.1.1 Set Up User Roles and Entitlement Policies

Every bank employee is mapped to an enterprise role. The enterprise roles are created in Oracle Internet Directory (OID) or equivalent Lightweight Directory Access Protocol (LDAP) store.

For handling business transactions, a user may need to be mapped to a set of services that are typically available to a single role. Such role is referred as the Application Role. Entitlements are defined on resources for the particular application role using Policy Management task. These entitlements drive the access privileges granted to the application role. For example, "perform" on an application service or "view" on a report resource.

Authorized personnel from the bank can use Oracle Directory Services Manager (ODSM) for OID maintenance.

A bank user can be mapped to multiple application roles. Each application role can be linked to its authorization policy within which coarse grained and fine grained authorization configuration can be done.

Examples of user access restrictions are as follows:

- Allow users without access restrictions to only view and select product groups classified as Office Accounts, once the user selects New Deposit from Landing page of Application Form during account opening process.
- Only allow users with access privileges to capture Office Account Ledger within the following list of tasks (maintenances or transaction) or common taskflows.

- All financial transactions where settlement mode is GL
- Miscellaneous General Ledger Transfer (Cash Deposit to GL)
- Cheque Deposit to GL
- Journal Multi Voucher Entry
- Product ledger Balance Inquiry
- Reconcile Office Accounts
- Payment or Collection Transaction
- Scan Reject
- CASA Backdated Transaction
- In the Common Settlement taskflow, one of the supported modes is GL, that is Ledger. Once this option is chosen, based on the branch, the system will allow the user to filter and select the appropriate GL to perform the transaction. From the picklist, the appropriate ledger code can be selected by the user.
- System provides a mechanism to define these entitlements or access policies that are to be maintained for the application roles applicable within the bank.

11.6.1.2 Transaction Blackout Configuration

Transaction Blackout typically is required when the bank wants to implement blackout or restrictions on the execution of certain maintenances or transactions. Such restrictions may be required for different business scenarios. A mechanism is provided to have user based blackout (combination of customer and application role) or total blackout for a particular transaction.

The dimensions on the basis of which the blackout details are maintained will typically include:

- Transaction (or application service)
- Channel (from where the request is initiated)
- Start Time (beginning of blackout date and time duration)
- End Time (end of blackout date and time duration)

Over and above this maintainable blackout, there is also a system enforced blackout during batch operations. There is a configuration by which the Banker Portal tasks can be allowed or disallowed during execution of batch processes. This is checked when the application service associated with the particular maintenance or transaction in the application is executed. An error message is displayed, if the blackout condition is met.

11.6.1.3 Origination Application Tracker Entitlements

The Application Tracker (Fast Path: OR100) within Origination enables users and customers to identify the progress with their particular application and to perform the necessary tasks or actions to ensure the application moves forward in the process. The ability to define the entitlements that are applicable for each user role is provided to the bank. The actions and options displayed within the Application Tracker take into account such entitlement definitions.

11.6.2 Approvals

Typically, the administration team within the bank configures the tasks for approvals as per the bank's credit, pricing, regulatory or other policies. Within the application, the approval configuration is to be done primarily on

the application service being executed corresponding to the task or business function being performed.

Artifact Dependency Map (ADM) is a mechanism provided to assert and identify the application services that are associated to a particular task or business function. The overridable business exceptions or reason codes associated with the application service can be configured for approval.

The application is pre-integrated with the Oracle SOA Suite for executing its business workflows. The Originations module uses several process or human workflow features to originate customers and accounts. The Approvals module makes use of the sophisticated participant assignment, routing or work-list features to fulfill the approvals use cases.

- The SOA suite identifies its users through authentication provider pointing to OID. The application UI and app servers also point to the same identity store to provide authentication rights to its users.
- Work-list users or process users are protected through access policies set up in OPSS. The SOA server domain is also re-associated to the same domain that the application UI and app-servers use to get the benefits of a centrally set up policy store.

Whenever a transaction is submitted by a user (banker, customer, and so on), security access check interceptors assert role-based access and fraud policies added on the service executed. Additionally, these interceptors also evaluate whether there are approvals configured on the service.

The output of these asserters is a decision on whether approvals are required or not. If approvals are required, the application executes the process (BPEL) configured for the transaction. Thereon, the BPEL process takes the responsibility of routing the approval task (work-item) to the configured assignees and ensuring that the assignees take the required action to complete the approval process.

Approval checks are of the following types:

- **Dual Control:** Any transaction can be set up for approvals (4-eyes principle).
- **User Limits:** User Limits assenter evaluates whether transaction amount is within limits available to the user (role).
- **Matrix Based:** Matrix assenter evaluates a matrix of facts available in the context of the transaction. This assenter is used to evaluate the delegated commitment authority and discretionary pricing facts.
- **Business Override Severity Configuration:** The severity configuration for the reason codes typically are as follows:
 - IGNORE
 - OVERRIDE
 - OVERRIDE - LOCAL (Local Authorization)
 - OVERRIDE _ RULES (This option provides the flexibility to maintain different entitlement rules per service and reason code combination)
 - REJECT
 - NOTIFY

This severity option can be configured differently for combination of dimensions like application role + branch + channel.

The approval task typically indicates to the approvers the following details:

- Request details including the initiator's user ID, and date and time when the request was initiated
- Business exception or reason code and its corresponding description
- View approver's history as part of the approval work-item
- Capture comments to indicate approval or rejection

Local Authorization provides a mechanism for the approver to action the approval request from the initiator's workstation, thereby saving time in remote access of the approval work item from the worklist. Typically, it is useful for scenarios like over-the-counter transactions where the number of users in physical branch are less.

Support for deferred approval is allowed for set of tasks and based on the preconfigured periods. The supervisor can approve the same and if no action is taken within the period, the task becomes void. The posting date of such transactions will change to the date on which the supervisor approves the transactions.

11.6.2.1 Matrix Based Authorization

This section explains the matrix based authorizations.

11.6.2.1.1 Pricing Approval Negotiations

Matrix based authorization are supported for different pricing dimension negotiations like:

- User Discretionary Margin (UDM)
- Fees
- Customized (base) rate capture
- Economic cost negotiation in servicing transactions like Term Deposit Redemption

This functionality is available for a wide range of transactions spanning Origination (for lending covering Loans and Overdraft) primarily as part of Structure Solution step, Loans (Actions within Manage Loan Account like Split Loan or Offer Swap OR Actions in Manage Facility Within Arrangement task like Add New Account respectively), and Term Deposit (Contract Modification or Fund Term Deposit).

The key difference at a high level between Origination and Non Origination approvals is that there is a Return task capability for origination approval rejections while this capability is available for servicing only in a limited set of tasks.

Different attributes are provisioned which can be used in rules for UDM or fee negotiation approvals. For example, Requested Amount and Product Group for a UDM negotiation approval while the Fee Negotiation details for Fee negotiation approvals. Also, generic attributes like business unit, transaction branch are available.

11.6.2.1.2 Credit Approval Negotiations

This functionality is for approval of credit for lending applications within the Origination process. Matrix attributes like aggregate application amount, sum of facilities being applied based on the Loan To Value (LTV) group, business unit and so on can be used to create different rules for getting the applications approved.

11.6.2.1.3 Collateral Processing Approvals

Configure approval matrix authorization for the following transactions in LCM module:

- Collateral Sub Division
- Collateral Consolidation
- Collateral Valuation

- Collateral Realization
- Release of Collateral

Common Attributes as well as certain specific attributes with respect to these transactions can be used for creating conditions for authorization rule within Policy Management task in the application as well as approval task assignment rules within Oracle SOA Suite.

11.6.2.1.4 Transaction Limit Checks

Flexibility is provided for transaction limits checks as part of Approval module for handling approval of:

- Daily or Cumulative limit checks for specific transactions
- Cumulative limit check for a group of transactions
- Specific override limits for a customer or account for handling exceptions to the transaction limit checks configuration

11.6.2.1.5 Cancel Pending Approval Request

Flexibility is provided to initiators to cancel their approval requests prior to the completion of the approval process. Currently, this option is available only to the initiator of the approval request. Another advantage of this capability is that when the Close Teller Batch fails due to approval requests pending completion, the initiator can cancel such requests and proceed with teller batch closure. Prior to this option being available, the initiator had no option but to pursue the required approvers to either approve or reject the requests.

11.6.2.1.6 Approval Process Tracking

The following capabilities are provided:

- View the status of the approval tasks associated with a particular request pending approval.
- View complete task history and state transitions for each of the approval tasks created.

Approval of Origination tasks can be tracked through the Application Tracker (Fast Path: OR100). The status of approval requests initiated from assisted or banker pages can be tracked through Work Item Inquiry (Fast Path: WL001).

12 Interface with other Master Data Management

This section describes the key features related with productized interface of Oracle Banking Party Management Functional Overview with Oracle Customer Hub (OCH). Similar capability is available, if Oracle Banking Party Management needs to integrate with any other MDM.

Key Features

- Capability to onboard a newly on-boarded customer or member to OCH first and then to Oracle Banking Party Management.
- Capability to update OCH first in the event of any updates to the party data.
- Capability to onboard (Quick Onboarding) an OCH customer in Oracle Banking Party Management through quick onboarding service.
- Capability to view and update the data captured in Oracle Banking Party Management based on the latest data from OCH.
- Capability to push the party data to OCH.