****

**Functional Specification Document (FSD)**

|  |  |
| --- | --- |
| Project ID |  |
| Project Name | Transact Enhancement R1V7 Phase 1 |
| Document Confidentiality |  |
| Document Status | Draft/ Final |
| Document Version | V2.0 |
| Document Date | 19 April 2017 |

Template Version: 2016-v1df

**Issue / Amendment Record**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Project ID** | |  | | | |
| **Project Name** | | FSD\_Transact\_R1V5 Phase 1 | | | |
| **Document Status** | | Draft / Final | | | |
| **Version** | **Date** | **Author** | **Reviewer** | **Approver** | **Version Summary** |
| 1.0 | 19 April 17 | Catherine Lam | Christian Arabia | Sharene Lim | First Draft, Enhancement detail for approval worksheet |
| 2.0 | 11 Aug 17 | Catherine Lam | Christian Arabia | Koh, Tat Hai | Add item 5 business Boundary |
|  |  |  |  |  |  |

**Table of Contents**

[1 Preamble [this section can be removed prior to submission] 6](#_Toc461804378)

[2 Document Presentation 7](#_Toc461804379)

[2.1 Document Purpose 7](#_Toc461804380)

[2.2 Document Intended Audience 7](#_Toc461804381)

[3 Project Overview 8](#_Toc461804382)

[4 Assumptions, Exclusions and Constraints 21](#_Toc461804383)

[5 Solution Architecture 22](#_Toc461804384)

[5.1 Architecture Overview 22](#_Toc461804385)

[5.2 Architecture Specifications 22](#_Toc461804386)

[6 Use Cases 23](#_Toc461804387)

[6.1 Use Case: (1) 23](#_Toc461804388)

[7 Functional Specifications 25](#_Toc461804389)

[7.1 Solution Requirements: (1) 25](#_Toc461804390)

[8 Report Requirements 26](#_Toc461804391)

[8.1 Report 001 <Report Name> 26](#_Toc461804392)

[8.1.1 Report 001 – Mockup 26](#_Toc461804393)

[8.1.2 Reporting 001 – Logic 26](#_Toc461804394)

[8.1.3 Reporting 001 – Fields 26](#_Toc461804395)

[9 Information Security Specifications 28](#_Toc461804396)

[9.1 Identity & Access Management (IAM) specifications 28](#_Toc461804397)

[9.1.1 Authentication and Single Sign On 28](#_Toc461804398)

[9.1.2 Access Request 28](#_Toc461804399)

[9.1.3 Access Provisioning 28](#_Toc461804400)

[9.1.4 Access Matrix Maintenance (Roles and Entitlements) 29](#_Toc461804401)

[9.1.5 System Generated Feed for User List 30](#_Toc461804402)

[9.1.6 Security Administration Audit Logging 30](#_Toc461804403)

[9.1.7 Self service password reset facility 30](#_Toc461804404)

[9.1.8 Account dormancy 30](#_Toc461804405)

[9.2 Monitoring and Response Specs 30](#_Toc461804406)

[9.3 Information Protection (IP) Specifications 31](#_Toc461804407)

[9.3.1 Protection of Data at Rest 31](#_Toc461804408)

[9.3.2 Protection of Data in Motion 32](#_Toc461804409)

[9.3.3 Protection of Data in Use 32](#_Toc461804410)

[9.3.4 Malware Protection 32](#_Toc461804411)

[9.4 Risk and Compliance Specs 33](#_Toc461804412)

[9.4.1 Risk Assessment 33](#_Toc461804413)

[9.4.2 Code Security Review 33](#_Toc461804414)

[9.5 Governance, Risk and Control Specifications 33](#_Toc461804415)

[9.6 Policy & Awareness Specifications 34](#_Toc461804416)

[10 Decommission Specifications 35](#_Toc461804417)

[11 Data Quality Specifications 36](#_Toc461804418)

[11.1 Data Quality Management 36](#_Toc461804419)

[11.1.1 Data Dictionary 36](#_Toc461804420)

[11.1.2 Data Sourcing and Transformation 36](#_Toc461804421)

[11.1.3 Controls and Exception Management 37](#_Toc461804422)

[11.1.4 Data Profiling 38](#_Toc461804423)

[11.1.5 Data Quality Monitoring and Governance 39](#_Toc461804424)

[11.1.6 Reference Data 39](#_Toc461804425)

[12 Screening Projects 40](#_Toc461804426)

[12.1 System Specification / Configuration 40](#_Toc461804427)

[12.2 Watch List 40](#_Toc461804428)

[12.3 Alert Management Process 40](#_Toc461804429)

[12.3.1 Alert Management Workflow 41](#_Toc461804430)

[12.3.2 Alert Management Requirements 41](#_Toc461804431)

[12.4 Escalation Matrices 41](#_Toc461804432)

[12.4.1 Escalation Matrices Representation 41](#_Toc461804433)

[12.4.2 Escalation Matrice Requirements 42](#_Toc461804434)

[12.5 Controls Setup 42](#_Toc461804435)

[12.6 Problem Management 42](#_Toc461804436)

[13 Appendices 44](#_Toc461804437)

[13.1 Reference Material 44](#_Toc461804438)

[13.2 Definitions and Acronyms 44](#_Toc461804439)

[14 Document History 45](#_Toc461804440)

[15 Document Reviews 46](#_Toc461804441)

[16 Document Approvals 47](#_Toc461804442)

[17 Performance Goals 48](#_Toc461804443)

[18 Application Overview 49](#_Toc461804444)

**Tables**

[Table 2—1 Intended Audience 7](#_Toc461804445)

[Table 4—1 Overall Assumptions 21](#_Toc461804446)

[Table 4—2 Overall Exclusions 21](#_Toc461804447)

[Table 4—3 Overall Constraints 21](#_Toc461804448)

[Table 5—1 Intended Audience 22](#_Toc461804449)

[Table 6—1 Use Case 1 Narrative 23](#_Toc461804450)

[Table 7—1 Solution Requirements 25](#_Toc461804451)

[Table 8—1 Solution Requirements 26](#_Toc461804452)

[Table 8—2 Report 001 - Header Fields 26](#_Toc461804453)

[Table 8—3 Report 001 - Fields 26](#_Toc461804454)

[Table 8—4 Report 001 - Trailer Fields 26](#_Toc461804455)

[Table 8—5 Report 001 – Delivery Requirements 27](#_Toc461804456)

[Table 9‑1 Spec – Authentication and Single Sign-On 28](#_Toc461804457)

[Table 9‑2 Spec – Access Request 28](#_Toc461804458)

[Table 9‑3 Spec – Access Provisioning 28](#_Toc461804459)

[Table 9‑4 Spec – Access Matrix Maintenance (Roles and Entitlements) 29](#_Toc461804460)

[Table 9‑5 Spec – System Generated Feed for User List 30](#_Toc461804461)

[Table 9‑6 Spec – Security Administration Audit Logging 30](#_Toc461804462)

[Table 9‑7 Spec – Self service password reset facility 30](#_Toc461804463)

[Table 9‑8 Spec – Account dormancy 30](#_Toc461804464)

[Table 9‑9 Spec - Monitoring and Response 30](#_Toc461804465)

[Table 9‑10 Spec - Protection of Data at Rest 31](#_Toc461804466)

[Table 9‑11 Spec - Protection of Data in Motion 32](#_Toc461804467)

[Table 9‑12 Spec - Protection of Data in Use 32](#_Toc461804468)

[Table 9‑13 Spec - Malware Protection 32](#_Toc461804469)

[Table 9‑14 Spec – Risk and Compliance 33](#_Toc461804470)

[Table 9‑15 Spec - Code Security Review 33](#_Toc461804471)

[Table 9‑16 Spec - Governance, Risk and Control 33](#_Toc461804472)

[Table 9‑17 Spec - Policy & Awareness 34](#_Toc461804473)

[Table 10—1 Decommission activities 35](#_Toc461804474)

[Table 11—1 (Sample) Requirements – Data Quality – Control and Exception Management 37](#_Toc461804475)

[Table 11—2 (Sample) Requirements - Data Profiling 38](#_Toc461804476)

[Table 11—3 Requirements – Data Quality Monitoring and Governance 39](#_Toc461804477)

[Table 12—1 System Specification / Configuration 40](#_Toc461804478)

[Table 12—2 Watch List 40](#_Toc461804479)

[Table 12—3 Alert Management Requirements 41](#_Toc461804480)

[Table 12—4 Escalation Matrice Requirements 42](#_Toc461804481)

[Table 12—5 Controls Setup 42](#_Toc461804482)

[Table 12—6 Problem Management 43](#_Toc461804483)

[Table 13—1 Reference Material 44](#_Toc461804484)

[Table 13—2 Definitions and Acronyms 44](#_Toc461804485)

[Table 14—1 Document History 45](#_Toc461804486)

[Table 15—1 Document Reviews 46](#_Toc461804487)

[Table 16—1 Document Approvals 47](#_Toc461804488)

[Table 18—1 Existing Functionality 49](#_Toc461804489)

[Table 18—2 Intended changes 49](#_Toc461804490)

[Table 18—3 New/Changed Interfaces 49](#_Toc461804491)

**Figures**

[Figure 1 Use Case 1 23](#_Toc461804492)

[Figure 2 Future Organisation Structure Business Unit (n) 41](#_Toc461804493)

[Figure 3 Future Organisation Structure Business Unit (n) 42](#_Toc461804494)

# Preamble [this section can be removed prior to submission]

Note to authors:

Input to this document:

* Project BRD

This document:

* is the source for the Solution Design
* represents requirements in a table format to facilitate requirements tracking from the project business requirements to testing
* must be signed off by the Project Manager and reviewed by the project Stakeholders

Output from this document:

* RTM
* Solution Design

For multiple phased projects: an FSD by project phase is required

For changes to this document after the document has been Finalized a CR must have been raised, updates to the BRD documented and the referenced CR included in the section References.

An audience guide is included in the Reviewers list as an example – please review it against the TOR

# Document Presentation

## Document Purpose

This document defines the functional specifications for Transact Enhancement R1V7 Phase1. It will be used as the basis for the following activities:

• Creating solution designs

• Developing test plans, test scripts, and test cases

Requirements not included in this document are out of scope for this project. Any change to requirements must be managed through the project’s Change Management process.

The purpose of this project is to cater for recent approved CRD and also policy refinement. This document defines proposed logic changes to facilitate the specific logic requirement of the above CRD and policy update in Transact by Transact SM and Transact Approval Worksheet in Transact Front End Application System respectively.

## Document Intended Audience

List the key stakeholders, include for each Stakeholder the -position and role in project refer to TOR. Include technology, test team and vendor (if applicable).

This document should be read by

Table — Intended Audience

| # | Name | Role / Capacity |
| --- | --- | --- |
|  | CoE - Retail Decision Systems  Leung, William Kin Pong | HK Transact SM |
|  | Chim, Rebecca Pui Pui & Liang, Tony | HK Transact Business Owner & Team: |

# Project Overview

This is a brief description of what the project is about. Information can be extracted from the PED or BRD.

This document is detailed the Transact Enhancement R1V7 phase 1 and its related Transact SM for Hong Kong only.

Table — Objectives

| # | Objective | Outcome measure |
| --- | --- | --- |
| 1 | i ) Long Tenor EBIL CRD | i) Proper approval level / line assignment / deviation code/ etc will be triggered |
| 2 | Policy Refinement on years of Experience of Owners | Proper approval level trigger in relation to years of experience of owners |
| 4 | L1 approval for age plus tenor > 65 years | Proper approval level trigger for age plus tenor > 65 years |
| 5 | Business Boundary | Approval level / deviation code/ etc will be triggered |

**Following are the requirements to be developed in this project:**

1. Additional of new program codes and reason codes to be adding in TRANSACT. Thus, it is requiring display the new program codes in approval worksheet under section Product Eligibility. [Item1.1]
2. GIL/GOD line assignment alignment in conjunction with policy refinement on years of experience of owner, it is require showing Level 1 and Level 3 under Section E. Financials in approval worksheet Credit Limit Section. [Item2]
3. Policy change on L1 approval for age plus tenor > 65 years, thus require update approval worksheet under age restriction section. [Item4]
4. Business boundary for Sales Turnover (STO) changes, thus require updating approval worksheet under Annual Sales Turnover. [Item 5]
5. Phase 1 development involve of update policy change in TRANSACT approval worksheet only.

## Scope Statement

| **Item** | **Details** | **Documents** | **Request Change in Transact** | **Change in scope at** |
| --- | --- | --- | --- | --- |
| **1** | Long Tenor EBIL CRD & Enhancement on existing Normal BIL with Tenor > 3 years |  | 1. **Long Tenor EBIL CRD**   **Product:** BIL only  **Creation of Program Code:** LongTenEBIL  **Program Code Description:** Long Tenor EBIL CRD  **Eligibility:**   * Customer Type: Sole Proprietorship/ Partnership/ Limited Companies * Min. Business Vintage: 3 Year * Max Tenor up to 5 years * Min. STO USD 1 Million * CG grade 10A or better (Up to 5 year tenor for CG9A or better) * -0.1<=LCR<=1.0x * For all other credit criteria not covering from above points, L2/L3 approval in accordance to current Normal BIL policy is allowed (Except LCR)   **Max Tenor:** 5 years  **MUE:**  Max MUE USD 300K (Same as E-BIL Program)  **Max Ticket Size:**   * Max Loan Amount up to HKD 2.0 Millions  |  |  | | --- | --- | | **Code** | **Description** | | ETJ3 | L3 – Not meet Program criteria: CV grade | | ETK3 | L3 – Not meet Program criteria: MUE | | ETL3 | L3 – Not meet Program criteria: Tenor | | ETM3 | L3 – Not meet Program criteria: Max. loan ticket size | | ETD3 | L3 - Not meet Program eligibility criteria: LCR | | ETC3 | L3 - Not Meet Program eligibility criteria: CG | | EGV3 | L3 - Stressed Industries |   **Campaign Code:**   * LongTenEBIL\_F   **Stressed Industries ISIC Table** | Transact SM change the logic based on condition in request change.  Transact Font End Application change the approval worksheet only. |
| **2** | GIL / GOD Line Assignment Alignment |  | |  |  | | --- | --- | | Existing | Proposed | | Max Loan Amount to Annual Sales Turnover Ratio for CG 5A – 9A  For BIL / BOD 25% (for positive LCR range, i.e., 0 <= LCR <= 1.5x); Else, 15% for LCR range from -0.1x to below 0  For GIL / GOD 15% within valid LCR range (i.e., -0.1x <= LCR <= 1.5x) | Max Loan Amount to Annual Sales Turnover Ratio for CG 5A-9A  For BIL\* / BOD/ GIL\*/ GOD 25% (for positive LCR range, i.e., 0 <= LCR <= 1.5x);  Else, 15% for LCR range from -0.1x to below 0  ~~For GIL / GOD 15% within valid LCR range (i.e., -0.1x <= LCR <= 1.5x)~~  \*The above alignment applies to EBIL & EGIL programs, and supersedes prevailing program specific requirement. | | For the other CG band (9B or below), loan assignment are aligned for all BB unsecured products, and no further action required. | |   **Relevant field in Transact System**  Optimal Amount of Line Assignment Matrix under Credit Analyst Summary    **Relevant field in Approval Worksheet**  Show under Level 1 and Level 3 under Section E. Financials in Approval Worksheet | Transact SM change the logic based on condition in request change.  Transact Font End Application need to ensure the value display accordingly at approval worksheet |
| **4** | L1 approval for age plus tenor > 65 years |  | |  |  | | --- | --- | | Existing | Revised | | Age Restriction at Time of Application for BIL/GIL   * Maximum age of sole proprietor / all partners / guarantors of limited companies plus tenor must be <= 65. * For **sole proprietorship** whereby his age plus tenor > 65 (currently under L3), application can be treated under L1 approval subject to:   + A successor is present for the business and this successor must be a family member of the sole proprietor; and   + The successor is actively involved in the business management of the sole proprietorship; and   + Successor’s age plus tenor <= 65; and   + Both sole proprietor and successor are jointly and severally liable for the debt.   Age Restriction at Time of Application for GOD/BOD   * For partnership and limited companies, at least 1 of the guarantors must be aged between 25 and 60 years old. All partners/business principals/directors/shareholders must be either personally liable for the debt or serve personal guarantees to the bank up to our satisfaction. * For **sole proprietorship** whereby his age >60, application can be treated under L1 approval subject to the above 4 sub bullet criteria except that successor’s age <= 60. | Age Restriction at Time of Application for BIL/GIL   * Maximum age of sole proprietor / all partners / guarantors of limited companies plus tenor must be <= 65. * If age plus tenor > 65 (currently under L3), application can be treated under L1 approval subject to:   + The presence of a successor**/additional guarantor**. For the case of sole proprietor, successor must be a family member of the sole proprietor; and   + The successor**/additional guarantor** is actively involved in the business management of the sole proprietorship/partnership/ limited company; and   + Successor’s**/additional guarantor’s** age plus tenor <= 65; and   + Sole proprietor, successor and **additional guarantor** are jointly and severally liable for the debt.   Age Restriction at Time of Application for GOD/BOD   * For partnership and limited companies, at least 1 of the guarantors must be aged between 25 and 60 years old. * All partners/business principals/directors/shareholders must be either personally liable for the debt or serve personal guarantees to the bank up to our satisfaction. * If his/her age > 60, application can be treated under L1 approval subject to the above 4 sub bullet criteria except that successor’s**/additional guarantor’s** age <= 60. |   Relevant deviation code for the above change (existing code):   |  |  | | --- | --- | | **Code** | **Description** | | AGE3 | L3 - Age Restriction >65 Yrs or <25 Yrs | | Transact SM change the logic based on condition in request change.  Transact Font End Application change the approval worksheet only |
| **5** | Business Boundary |  | Deviation Code L3 / L5 deviation code will be triggered for the following scenarios:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Scenario | Product Type | Customer Type | STO | Deviation Code | | 1 | BIL | NTB/ETB | >USD15M | L5 | | 2 | Bundle BIL / BOD | NTB/ETB | >USD15M | L5 | | 3 | Bundle BIL / BOD | NTB/ETB | >USD15M | L5 | | 4 | GIL | NTB/ETB | >USD15M and ≤USD25M | L3 | | 5 | GIL | NTB/ETB | >USD25M | L5 |   For STO≤USD15M, approval level will be L1 for any product type and customer type.  Data will be stored and downloaded to Daily Data dump for Country MIS purpose. | Transact SM change the logic based on condition in request change.  Transact Font End Application change the approval worksheet only |

# Functional Description

## Function 1 – AIP Normal BIL Top Up Program CRD

### Description

Additional of new program codes [LongTenEBIL], Program Code Description [Long Tenor EBIL CRD], campaign code [LongTenEBIL\_F] and reason codes as per below table 1 for Product BIL only. Show the new program codes in approval worksheet under section Product Eligibilty. It is applicable for Product: BIL only.

**Table 1: Campaign Code:**

|  |  |
| --- | --- |
| **Code** | **Description** |
| ETD3 | L3 - Not meet Program eligibility criteria: LCR |
| ETC3 | L3 - Not Meet Program eligibility criteria: CG |
| EGV3 | L3 - Stressed Industries |
| **Code** | **Description** |
| ETJ3 | L3 – Not meet Program criteria: CV grade |
| ETK3 | L3 – Not meet Program criteria: MUE |
| ETL3 | L3 – Not meet Program criteria: Tenor |
| ETM3 | L3 – Not meet Program criteria: Max. loan ticket size |
| ETD3 | L3 - Not meet Program eligibility criteria: LCR |
| ETC3 | L3 - Not Meet Program eligibility criteria: CG |
| EGV3 | L3 - Stressed Industries |

### Screen Layout

1. i) Long Tenor EBIL CRD

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section** |  |  | | | |
| **Current Value** | | **L1** | **L3** | **Approval Level** |
| Product Eligibility | Program Code: LongTenEBIL | | * Customer Type: Sole Proprietorship/ Partnership/ Limited Companies * Min. Business Vintage: 3 Year * Max Tenor up to 5 years * Min. STO USD 1 Million * CG grade 10A or better (Up to 5 year tenor: CG 9A or better) * -0.1<=LCR<=1.0x | In case of any not meet eligibility criteria, return L3;  Display deviation reason description | Highest approval level to be displayed, e.g., L3 |

### Special Conditions

N/A

### Database Stored Procedure

1. sp\_html\_to\_word\_approval\_worksheet\_sel#app\_id#HK.sql
2. udf\_GetApprWorkSheetSCBBankingRelationshipInfo.sql

### Approval worksheet files

1. rpt\_html\_to\_word\_approval\_worksheet(HK).asp

### Transact design studio Screen changes

## Function 2 – GIL/GOD Line Assignment Alignment

### Description

This section is to update the logic in GIL/GOD Line Assignment Alignment. Change of current existing policy in Transact SM and the output its value at “Optimal Amount of Line Assignment Matrix” under Credit Analyst Summary SM section. There is no change at approval worksheet. However, SME-T require to ensure the output of Transact SM display at approval worksheet accordingly after transact SM change the logic.

### Screen Layout

2) GIL / GOD Line Assignment Alignment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section** |  |  | | | |
| **Current Value** | | **L1** | **L3** | **Approval Level** |
| **Credit Limit** | [No change is needed] | | [No change is needed]  (based on Optimal Loan Amount of Line Assignment Matrix for the new logic) | [No change is needed]  (based on Optimal Loan Amount of Line Assignment Matrix for the new logic) | Highest approval level to be displayed, e.g., L3 |

### Special Conditions

N/A

## Function 3 – L1 approval for age plus tenor >65

### Description

Revise the logic of age restriction at time of application for BIL/GIL. Transact SM returns reason code “AGE3” to transact front end application if L3 age restriction > 65 Years or <25 Years”. The changes should reflect in approval worksheet under section Age Restriction.

### Screen Layout

1. L1 approval for age plus tenor > 65 years

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section** |  |  | | | |
| **Current Value** | | **L1** | **L3** | **Approval Level** |
| **Age Restriction** |  | | >= 25 & <=65 (with Tenor) or (with successor/additional guarantor) | <25 / >65 (with Tenor) | Highest approval level to be displayed, e.g., L3 |

### Special Conditions

N/A

## Function 4 – Business Boundary

### Description

Revise the cut over of STO for product type: BIL, Bundle BIL/BOD, and GIL; customer type: NTB/ETB. It impacts to the approval level for the mentioned product type based on cutover STO. Thus, it is require to update transact approval worksheet for Annual sales turnover L3 display message.

### Screen Layout

1. Business Boundary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section** |  |  | | | |
| **Current Value** | | **L1** | **L3** | **Approval Level** |
| **Annual Sales Turnover** | [No change is needed] | | [No change is needed] | BIL /  Bundle BIL / BOD / Standalone BOD (for both NTB and ETB):  >117M – L5  GIL (NTB):  >117M to ≤195M – L3 with NOC  GIL (ETB):  >117M to ≤195M – L3 without NOC  GIL (for both NTB and ETB):  >195M – L5 | Highest approval level to be displayed, e.g., L3 |

### Special Conditions

N/A

# Assumptions, Exclusions and Constraints

List the major assumptions and constraints on the specifications

Table — Overall Assumptions

|  |  |  |
| --- | --- | --- |
| # | Item | Description |
| OOA-100 |  |  |
|  |  |  |

Table — Overall Exclusions

|  |  |  |
| --- | --- | --- |
| # | Item | Description |
| OAE-100 |  |  |
|  |  |  |

Table — Overall Constraints

|  |  |  |
| --- | --- | --- |
| # | Item | Description |
| OAC-100 |  |  |
|  |  |  |

# Solution Architecture

This is a refinement of what is stated in the respective Architecture Document. Reference material from there where practical.

Follow agreed diagram conventions for the domain in which this solution falls to ensure ease of understanding of change.

## Architecture Overview

Add detailed solution architecture if required.

* Include data mapping and data flow for each system and application feed, including data mapping for the system conversion and system flow schematic
* Include source systems
* Interface File Definition
* Etc

<provide details here>

## Architecture Specifications

Interface file definition, workflows, data mapping must be linked to a Functional Specification. BRD Ref can be n/a

Table — Intended Audience

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
|  |  |  |

# Use Cases

Use Cases

< A Use Case captures the required system behavior from the perspective of the end-user in achieving one or more desired goals. A use case diagram provides a high-level description of what your system should be able to do and who/what will interact with it.

## Use Case: (1)

Each Use Case should be documented following the structure in this template sub-section.



Figure Use Case 1

Table — Use Case 1 Narrative

| Item | Details |
| --- | --- |
| Use Case ID: | 1.1  <Unique identifier |
| Use Case Name: | View Alert  <Name must be unique, concise and reflect the task to be done by the user or system. Name should have a verb and a noun |
| Description: | Users must be able to review and alert  <Provide a brief description of the reason for and outcome of this use case |
| Actors: | User, System  <List the actors involved in the use case |
| Preconditions: | User has access to the system  Screening solution has generated an alert  <List any activities that must take place, or any conditions that must be true, before the Use Case can be started. |
| Trigger(s): | Alert message generated  <Action that occurs that starts the basic flow of the use case |
| Basic Flow: | Users view alert by accessing the alert form the Alert list screen  User access tab details  User access tab transactions  User closes alert screen  <The basic flow is the events of the use case when everything is perfect. |
| Alternate Flow(s): | n/a  <Alternate flow is something that causes a deviation from the basic flow |
| Postconditions: | Alert is ready for closure  <Describe the state of the system at the conclusion of the use case. |
| Notes: |  |

# Functional Specifications

Requirements must be unique, clear/concise, unambiguous, correct, testable, complete and traceable.

Add the Functional Specifications using the Table format highlighted below. When the requirement refers to a Use Case, add the Use Case number at the end of the requirement text, for example (Use Case #1)

Functional requirements from the BRD identified as “Must Have” and “Could Have” that have been agreed upon for this project delivery must be included in this document and detailed. There should be at least a 1 to 1 relationship between BRD functional requirements and requirements in this document.

Add Functional Specifications section as needed.

## Solution Requirements: (1)

This section might be split in several subsections for grouping the requirements as needed.

Data field mapping to input/output systems need to be documented and attached to a requirement

Data input/output validation must be included as well as requirement – what field is validated, what should happen if the validation is not successful, what should happen if the validation is successful

Include frequency of data load if applicable

Table — Solution Requirements

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
|  |  |  |

# Report Requirements

Short descriptions by report including what will the report be used for and by who.

If the report is provided by the solution with no change, the mock-up, logic, fields is not required but a copy of the report must be attached. Section “Delivery Requirements” is still required.

If this is an existing report being modified, a mock-up needs to be attached and only CHANGES to the report identified in the Logic and Fields section. Section “requirements” is required.

## Report 001 <Report Name>

Short report description including what will the report be used for and by whom.

<Description goes here>

### Report 001 – Mockup

Include a report mock-up including header, detail (4 or 5 lines) and the footer

<Mockup goes here>

### Reporting 001 – Logic

....

Table — Solution Requirements

| # |  |  |
| --- | --- | --- |
| Group BY | <Add group by fields> |  |
| Filter BY | <Add required filters if applicable> |  |
| Sort BY | <Add data sorting order> |  |

### Reporting 001 – Fields

Table — Report 001 - Header Fields

| Field Name | Field Definition | Field data format | Field length | Comment |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

Sample given in below table is for integrity purposes. Replace/Complete as per specific needs.

Table — Report 001 - Fields

| Field Name | Field Definition | Field data format | Field length | Comment |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Sample given in below table is for integrity purposes. Replace/Complete as per specific needs.

Table — Report 001 - Trailer Fields

| Field Name | Field Definition | Field data format | Field length | Comment |
| --- | --- | --- | --- | --- |
| Record count |  |  |  |  |
| Page number |  |  |  |  |
| End | END |  |  |  |

Requirement samples provided in below table. Replace/Complete as needed.

Table — Report 001 – Delivery Requirements

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
| BRE-001 | FR1-001 | The reports must be generated by EOD Batch, Monday to Friday excluding Singapore business holidays |
| BRE-001 | FR1-002 | The report must be generated on demand |
| BRE-001 | FR1-003 | The reports must be generated on demand only by users with “\_\_\_” access |
| ... | ... | The reports must be saved automatically in the folder \_\_\_\_\_\_\_ |
|  |  | The reports must be generated if no data should be included |
|  |  | The report must be generated in \_\_\_ format |
|  |  | The report must be printable |

# Information Security Specifications

## Identity & Access Management (IAM) specifications

Describe the specifications for authentication, single sign on, access requests, provisioning, roles and entitlements, generation of security reports, log of administrator activities and password reset.

**If the project/enhancement is for an existing system and if there are no changes to be implemented capability in regards to Information Security or if a section is not applicable for a new system**, then

* declare this here or in the section which has no change from current implementation (if considered not applicable for a new system, describe why)
* provide reference to current capability documentation

Specification guidance in the tables can be removed as required once specs have been written.

### Authentication and Single Sign On

Table ‑ Spec – Authentication and Single Sign-On

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-101 | FSS-101 | Active Directory and LDAP and the Bank's directory services. Refer to the decision tree defined by Group Architecture for authentication method in the [guidance](http://teamsites.sc.com/sites/TG/SP/PROC/SDF/Templates/Information%20Security%20Requirements%20–%20Systems%20Delivery%20Framework.pdf) and describe the mode selected for your application along with functional specs. Note: One or more options must be selected based on the authentication model. In case of additional requirements, choose others and provide details.    <details> |

### Access Request

Table ‑ Spec – Access Request

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-101 | FSS-201 | Design a formal request form with an approval workflow to request access to the system. It must identify the Bank ID of the individual who needs access to the system. This form must include the permissions (roles / entitlements) required to access.  <details> |

### Access Provisioning

Table ‑ Spec – Access Provisioning

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-301 | FSS-301 | Determine whether automated provisioning is feasible through the Bank’s standard provisioning solution. The system must integrate with web services for the request details to be consumed by the target system to provision the accounts with roles / entitlements and supplementary data. An end user account must be a BankID otherwise a separate reference must exist to reflect the owner of the account. The facility must also include the request reference number.  <details> |
| BSR-302 | FSS-302 | If automated provisioning is not feasible, for manual provisioning, design an interactive facility for administration of accounts with roles / entitlements and supplementary data. An end user account must be a BankID otherwise a separate input must exist for the administrator to reflect the owner of the account. The facility must also include an input to reflect the request reference number.  <details> |

### Access Matrix Maintenance (Roles and Entitlements)

Table ‑ Spec – Access Matrix Maintenance (Roles and Entitlements)

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-401 | FSS-401 | Determine whether automated provisioning is feasible through the Bank’s standard provisioning solution. The system must integrate with web services for the request details to be consumed by the target system and provisioning the account with roles / entitlements and supplementary data.  If automated provisioning is not feasible, for manual provisioning, design an interactive facility for administration of accounts, roles / entitlements and supplementary data. An end user account must be a BankID otherwise a separate input must exist for the administrator to reflect the owner of the account. The facility must also include an input to reflect the request reference number.  <details> |
| BSR-402 | FSS-402 | Determine the approval workflow for authorisation of roles and entitlements before they are provisioned onto the system.  <details> |
| BSR-403 | FSS-403 | Determine the interactive roles for use by business, support and administration  <details> |
| BSR-404 | FSS-404 | Determine the non-interactive roles for use by service accounts, batch jobs, etc.  <details> |
| BSR-405 | FSS-405 | Segregate the roles designed for admins and others making them mutually exclusive  <details> |
| BSR-406 | FSS-406 | Determine the appropriate entitlements to be granted to each role.  <details> |
| BSR-407 | FSS-407 | Ensure no single role provides access to conflicting functions (e.g. front/back office)  <details> |
| BSR-408 | FSS-408 | Ensure the roles reconcile with those in access request forms and the certification facility  <details> |
| BSR-409 | FSS-409 | Provide for a role certification facility for business owners on a periodic basis with all the details of roles and their entitlements.  <details> |

### System Generated Feed for User List

Table ‑ Spec – System Generated Feed for User List

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-501 | FSS-501 | Provide a mechanism to generate user list with the following attributes.  This is required for extraction of role and last login information for certification purposes; and for reconciliation of accounts provisioned in the target systems with approved requests (RMS) and those reflected in the certification system (MAR).  <details> |
|  |  |  |

### Security Administration Audit Logging

Table ‑ Spec – Security Administration Audit Logging

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-601 | FSS-601 | Log of all security administration activity such as Role/User Id creation, modification and deletion in a csv/txt log file with the following details at a minimum.    <details> |
| BSR-602 | FSS-602 | Provide details on how to integrate the audit logs with Splunk for monitoring of security administration activities.  <details> |

### Self service password reset facility

Table ‑ Spec – Self service password reset facility

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-701 | FSS-701 | For applications not authenticated by AD/LDAP, design a self service password reset facility  <details> |

### Account dormancy

Table ‑ Spec – Account dormancy

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-801 | FSS-801 | Application should develop functionality to enable account dormancy process. Please refer to the SCB GIS dormancy policy for latest requirements (e.g. disable/de-activate account after 90 days of inactivity).  <details> |

## Monitoring and Response Specs

The standard build for servers include the system components required to detect host intrusion, unauthorised database activity, insecure access to servers and for centralised logging. In this section, describe the requirements for response to unauthorised access detected on your servers and the need to review the standard logging configuration on the servers and the changes required, if any.

Table ‑ Spec - Monitoring and Response

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
|  |  | Define how an unauthorised event will be triggered and responded to |
| BSR-901 | FSS-901 | * On Symantec CSP agents on hosts as part of host intrusion detection solution (HIDS)   <details> |
| BSR-902 | FSS-902 | * On Imperva agents on databases as part of database activity monitoring (DAM).   <details> |
| BSR-903 | FSS-903 | * When accessing using Balabit appliances as part of session activity monitoring (SAM).   <details> |
| BSR-904 | FSS-904 | Determine how the events will be configured and logged and forwarded to a consolidated facility for review (using Splunk forwarding agents).  <details> |

## Information Protection (IP) Specifications

Describe the specific requirements for encryption, firewall rules, malware protection and data centric controls for data at rest, data in motion and data in use, as part of the technology standard solutions with GIS.

### Protection of Data at Rest

*The system must fulfill the following requirements for protection of data at rest.*

Table ‑ Spec - Protection of Data at Rest

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-1001 | FSS-1001 | Determine how logins, data storage, backups, log files and communication between the Group and its consumers will be encrypted.  <details> |
| BSR-1002 | FSS-1002 | Determine how the encryption will be used to secure login credentials, including transmit to/from the network device  <details> |
| BSR-1003 | FSS-1003 | Determine how encryption algorithms will be implemented (Symmetric Encryption, Asymmetric Encryption, Message Digest)  Equivalent or greater than AES- 128 bits (256 bits preferred), IDEA 128 bits, RC6 128 bits, Two fish 128 bits, Blowfish 128 bits,  CAST – 256 bits.  Equivalent or greater than 2048-bit RSA, ECC 160 bits, PGP/GPG-1024 bits (2048 preferred), TLS, AUTACK-1024 bits.  SHA-2 Family or above  <details> |
| BSR-1004 | FSS-1004 | Determine how digital signatures will be produced and used for protection of origin and authenticity. Business Owner must include contractual and evidentiary relevance of the digital signatures produced within the local legal and regulatory jurisdiction  <details> |
| BSR-1005 | FSS-1005 | Determine how the cryptographic keys will be rotated at regular intervals with a frequency not exceeding 10 years & ensuring operational stability. A higher frequency may be determined by the product/process owner.  <details> |
| BSR-1006 | FSS-1006 | Determine how encryption will be used for File Transfer across or external networks using PGP or equivalent, with appropriate key exchange procedures.  <details> |
| BSR-1007 | FSS-1007 | Mobile Apps: Determine how information stored on mobile devices will be secured by way of containerization and managed by Group Mobile Device Management. On-boarding must follow Enterprise Mobility Group (EMG) process.  <details> |

### Protection of Data in Motion

*The system must fulfill the following requirements for protection of data in motion.*

Table ‑ Spec - Protection of Data in Motion

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-1101 | FSS-1101 | Determine how DMZ proxy requirements for Bank’s systems accessing external systems will be implemented; this applies for both in-bound and out-bound connections  <details> |
| BSR-1102 | FSS-1102 | Determine how channels for external connections (VPN, SSL/TLS etc) will be secured  <details> |
| BSR-1103 | FSS-1103 | Determine the ports that must be restricted for connections from external sources  <details> |
| BSR-1104 | FSS-1104 | Determine the list of firewall rules with ownership information  <details> |
| BSR-1105 | FSS-1105 | Determine the bandwidth requirements with Networks team, if applicable  <details> |

### Protection of Data in Use

*The system must fulfill the following requirements for protection of data in use.*

Table ‑ Spec - Protection of Data in Use

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-1201 | FSS-1201 | Determine how sensitive data elements will be protected using access restrictions and encryption (where applicable) to prevent unauthorized access. Access to such data must be actively monitored  <details> |
| BSR-1202 | FSS-1202 | Determine how sensitive or confidential data will be protected using secure communication channel for transmission across systems. Legal and regulatory requirements around handling of sensitive information such as PII/NPI/Private data as applicable for the geographies/regions should also be considered.  <details> |
| BSR-1203 | FSS-1203 | Complete the data classification exercise and determine the appropriate level of controls that must be implemented for securing the data stored, processed and transmitted by the application.  <details> |

### Malware Protection

*The system must fulfill the following requirements for malware protection.*

Table ‑ Spec - Malware Protection

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-1301 | FSS-1301 | Symantec Enterprise Protection and Cisco Web Security product solutions are part of the ISO standard build.  Describe the services that must not be blocked; e.g - external connections established with third party entities through the Bank’s PSAC channel (that is through proxy devices); client services like SMTP, POP3, IMAP, or any such messaging protocol designed to send notifications or alert emails to customers.  <details> |

## Risk and Compliance Specs

Describe the specifications to complete risk assessment including third party (if applicable), requirements to demonstrate compliance to technical standards and for conducting security acceptance test, vulnerability assessment, penetration testing and code security review, as applicable with GIS.

### Risk Assessment

Table ‑ Spec – Risk and Compliance

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-1301 | FSS-1301 | Determine the controls to be implemented to mitigate the risks identified through Application Security Risk Assessment using [Riskwise](https://scbukeualtvip.intranet.standardchartered.com/riskwise/RWC/login/doLogOut)  <details> |
| BSR-1303 | FSS-1303 | Determine the controls to harden security configuration to be in line with High Level Technical Security Standards (HLSTS)  <details> |

### Code Security Review

Table ‑ Spec - Code Security Review

|  |  |  |
| --- | --- | --- |
|  |  |  |
| BRD Ref | FSD Ref | Specification |
| BSR-1401 | FSS-1401 | Determine the timelines and resources to resolve or mitigate the vulnerabilities identified through Code Security Review for high risk applications (e.g. Internet facing in Channels, Payments, FM), for protection against Open Web Application Security Project ([OWASP](https://www.owasp.org)) Top 10 vulnerabilities and [SANS top 25 programming errors](http://www.sans.org/top25-software-errors/#cat1).  <details> |

## Governance, Risk and Control Specifications

Describe the specification to complete asset risk assessment needed to demonstrate that all operational risks and residual security and technology risks will be documented and signed off by the business owner prior to going live.

Table ‑ Spec - Governance, Risk and Control

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-1701 | FSS-1701 | Document all operational and residual security & technology risks and get it signed off by the business owner before application goes live. Any risks that are planned to be addressed must be periodically reviewed for tracking and closure.  <details> |

## Policy & Awareness Specifications

Describe the specifications to comply with policies, procedures, standards and guidelines available in the Control Framework Library with GIS

Table ‑ Spec - Policy & Awareness

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BSR-1801 | FSS-1801 | Determine compliance to the policies, procedures, standards and guidelines available in the [Control Framework Library (CFL)](http://teamsites.sc.com/sites/gis/gisprd/rm/Control%20Framework%20Library/Control%20Framework%20Library.aspx?PageView=Shared). Any deviations must be tabled at the appropriate risk governance forum for review and assessment.  <details> |

# Decommission Specifications

Add decommissioning activities for cases where the project/change requires it.

Table — Decommission activities

| BRD Ref | FSD Ref | Specification |
| --- | --- | --- |
| BDC-001 | NDC-001 |  |
| ... | ... |  |
|  |  |  |
|  |  |  |

# Data Quality Specifications

This section applies to Businesses, Functions, Systems and Processes (and associated programs and projects in the same) which have agreed to be in compliance with the Data Quality Management policy of the Bank.

For guidance on the same, please reach out to the Data Governance & Policy team via [Data Governance & Policy](mailto:DataGovernance&Policy?subject=Query%20on%20SDF%20Artefact:) email ID or refer the Chief Data Officer Bridge site for guidance.

This section specifies the characteristics of data required for the project to meet its objectives. This covers:

* Metadata specifications (data dictionary) including data profiling (if relevant),
* Data sourcing and transformation (including mapping of the functional requirements to business requirements)
* Controls and exception management processes in place to ensure quality expectations are met
* Data quality management and governance

This section also covers the controls / procedures / Key Risk Indicators to ensure the data is suitable for the stated purpose on an ongoing basis.

**All sub-sections are mandatory**. In the event a particular sub-section is not applicable, there must be a concise explanation as why it is not applicable.

## Data Quality Management

### Data Dictionary

This is an extension of section 7.2 Data Elements as per the Business Requirements Definition document template.

Document the information (or metadata) about the critical data elements either originated/transformed/derived in source systems or used/consumed in downstream processes/systems as part of this project. This is important to validate and ensure the critical data elements are clearly understood by both the data provider and data consumer in terms of its creation and usage respectively.

The Data Dictionary template from that completed in the Business Requirements Definition document must to be used to ensure continuity – – this is available from the [Data Governance Bridge page](https://thebridge.zone1.scb.net/docs/DOC-51819). A guide on how to complete this template is available on the same Bridge page.

The completed template / data dictionary will also be reviewed for accuracy, relevance and adherence to the Metadata standards and will be loaded into the bank’s Group Data Dictionary (Business Glossary) to create an integrated group data taxonomy of critical data elements.

**Note**- Refer to the Group data dictionary (the link to the Business Glossary is available via the [Data Governance Bridge page](https://thebridge.zone1.scb.net/docs/DOC-51819)) to read and re-use the description and associated information of critical data elements (if relevant to your project) that have already been documented from prior projects

<use referenced template for this section or state why the section is not applicable>

### Data Sourcing and Transformation

This section maps out how the data domain / data elements outlined as per Business Requirement Definition document template sections 7.1 and 7.2 will be sourced and made ready for consumption.

This section will state the sources of data, including the application instance and table name and for each data element, describe how the data will be extracted, transformed, delivered and verified and made ready for consumption. This section must state amongst other aspects:-

* State the translation rules, especially where content from source system is mapped to values on the target system. Also to describe the transformation rules, along with any derivation logic required.
* Ensure there is a “catch all” mechanism to trap unexpected values, with suitable exception management processes. Where applicable, use designated golden sources for reference data.
* Specify the basis and process for merging related data from multiple sources (e.g., a client’s data and postings from EBBS with the relevant payment transaction from dotOpal)
* Define the granularity for master data (e.g., sub-profile level or profile level information from SCI; global identifiers or market level identifiers for securities). This will help specify the join conditions for combining with transaction data or for merging with related data from other sources.
* Describe the criteria for successful validation and state how validation failures will be handled and communicated back to the source

In cases where the business requirements are simple and clearly stated in the Business Requirements Definition document - there is no need to restate them here (a reference to the relevant BRD section will suffice).

**Note (1)** – **the prescriptive templates to use are listed below** (in the absence of any existing artefacts / documents that hold the same information to similar level of detail)

* D2 and D6 – Data Interface & Transformation Logic template (this is available from the [Data Governance Bridge page](https://thebridge.zone1.scb.net/docs/DOC-51819)). A guide on how to complete this template is available on the same Bridge page.

**Note (2)** – the above information may also be contained within an Interface Specification Document.

<use referenced template for this section or state why the section is not applicable>

### Controls and Exception Management

This is an extension of section 7.3 Data Quality Expectations and Controls as per the Business Requirements Definition document template- for each critical data element identified for this project, this section is to:-.

* Specify the minimum controls that will be set in place to meet the quality expectations outline as per the Business Requirements Definition document template section 7.3
* Identify any potential failure points associated with the data sourcing / transformations / derivation and specify the minimum controls to be set-in place to meet the quality expectations.
* Identify and state the possible exceptions that may surface and the associated exception management processes.
* **Note (1)** – the **prescriptive templates to use is the Data Quality Controls template**, in the absence of any existing artefacts / documents that hold the same information to similar level of detail (this is available from the [Data Governance Bridge page](https://thebridge.zone1.scb.net/docs/DOC-51819)).
* **Note (2)** – Please complete the Data Quality Controls template in conjunction with the prescribed list of controls outlined in the DQMF Operational Risk Framework (ORF) Controls (this is available from the [Data Governance Bridge page](https://thebridge.zone1.scb.net/docs/DOC-51819)).
* For each exception, describe how it will be handled, including where it will be logged, the parties that will be alerted to the exception, any workaround that can be triggered to progress the data flow while the exception is being handled, and controls to ensure that all exceptions are closed within a particular period. State whether a SLA or similar contract is required to ensure timely closure of all exceptions

Table — (Sample) Requirements – Data Quality – Control and Exception Management

| No | Data Elements / Source Eleets | Quality Expectations / Control Failure Points | Minimum Controls | Expectation Management Process / ORF Process Name |
| --- | --- | --- | --- | --- |
| E.g. | Customer name (first, middle and last) | * In UK English only * daily refresh from customer master * no special characters * first / middle / last name in separate columns | * Daily reconciliation with client master * Validation checks in ETL layer for special characters and language * Separate mandatory columns for first/middle/last names at client on-boarding process * Specific DQ metrics to monitor each quality element | * Client Data Exception Process * ORF Process - Client Static Data Management |
|  |  |  |  |  |

<use referenced template for this section or state why the section is not applicable>

### Data Profiling

**Note** – this section is only required for Business/Function projects where meeting the quality requirements of the data consumer is **central and essential** to the effectiveness of the Business/Function’s process and operating requirements OR to meet specific regulatory requirements.

This is an extension of section 7.2 Data Elements and 7.3 Data Quality Expectations and Controls as per the Business Requirements Definition document template – for each critical data element identified for this project, this section is to profile the source data if they meet the specific quality requirements of the project – this includes:-

* compare the source data’s data definitions with its actual data - to help ensure that the data definitions are understood correctly and to verify whether said data attributes are being used as intended
* understand the current state of data quality – this includes validate completeness and uniqueness of key attributes, check % population of core attributes and verify validity of core attribute values.
* identify standard reference data candidates - to check if reference data attributes are existing enterprise data available on RDM. If yes, subscription from RDM should be considered

This section’s output will then tie back the results of the data profiling exercise to Section 12.1.3 Controls and Exception Management section and Section 12.1.5 Data Quality Monitoring and Governance section here in this Functional Specification document, to manage any existing shortfall in meeting data quality requirements.

Table — (Sample) Requirements - Data Profiling

| No | Data Elements | Quality Requirements | Data Profiling Results | Outcome |
| --- | --- | --- | --- | --- |
| E.g. | Customer name (first, middle and last) | * In UK English only * daily refresh from customer master * no special characters * first / middle / last name in separate columns | * Names in Mandarin (non-English noted) * Special Characters noted for UK & Malaysia client static * Full names are documented in first name column for Singapore | * ETL business rules in place to translate Mandarin to English UK (CLOSED) * Special characters – JIRA raised and being addressed by UK/Malaysia Retail Ops (OPEN) * Full names in 1st column – JIRA raised and being addressed by SG Retail Ops (OPEN) |
|  |  |  |  |  |

**Note** – (1) The Data profiling activity should be done as part of the Elaboration (or Architecture & Design) stage of the System Delivery Framework (2) Any systemic gaps in meeting data quality requirements outlined in the Business Requirement Definition document should be raised and logged as a data quality issue in the Bank’s issue tracking processes (e.g. JIRA, REMEDY, etc) for remediation. (2) Further guidance on methods and tools to perform Data Profiling is available on the CDO Bridge via the [Data Governance Bridge page](https://thebridge.zone1.scb.net/docs/DOC-51819)).

<use referenced template for this section or state why the section is not applicable>

### Data Quality Monitoring and Governance

This is an extension of section 7.4 Data Quality Monitoring as per the Business Requirements Definition document template and revalidated / enriched with the results of data profiling (where applicable).

This section details how the key quality criteria for the critical data elements originated / transformed / transmitted / consumed as part of this project will be monitored for its quality parameters and agreed thresholds. The data quality dimensions to be evaluated, mechanism for evaluation, tolerances, actions to be taken for breaching tolerances and closure of any breaches will be specified here

Table — Requirements – Data Quality Monitoring and Governance

| No | Data Elements | Quality Requirements | Data Profiling Results | Outcome |
| --- | --- | --- | --- | --- |
| E.g. | Customer name (first, middle and last) | * < 2% difference from client master * < 5% special character | * Automated customer static report from client static master * Weekly / Business DQ Forum | Client On-boarding (Process ID # XXX) |
|  |  |  |  |  |

**Note** – if the table above is not sufficient, document separately and attach in excel template here.

### Reference Data

The Business Requirements Definition and the data profiling results will state the reference data requirements. The identification of data elements as reference data, establishing the right sources for the data and setting up new elements in the reference data platforms are specified in this section. The treatment is similar to other data items to the extent of validations, transformations and exception management, with appropriate controls.

**Note** – **the prescriptive templates to use are listed** below (in the absence of any existing artefacts / documents that hold the same information to similar level of detail)

* D5 – Master Reference Data Mapping (this is available from the [Data Governance Bridge page](https://thebridge.zone1.scb.net/docs/DOC-51819)).). A guide on how to complete this template is available on the same Bridge page.

<use referenced template for this section or state why the section is not applicable>

# Screening Projects

**Remove this section if the project is not a screening project**

## System Specification / Configuration

Include in FSD system specification / configuration (system logic, algorithms, confidence levels, thresholds setting, alerts, parameters and rules)

Include frequency of data load

Include frequency of screening.

Table — System Specification / Configuration

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
| ... | FSP-001 |  |
| ... | ... |  |
|  |  |  |
|  |  |  |

## Watch List

Screening projects – Include the Watch List to be used. Frequency of WatchList refresh. Frequency of screening against specified WatchList.

Table — Watch List

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
| BWA-001 | FWA-001 |  |
| ... | ... |  |
|  |  |  |
|  |  |  |

## Alert Management Process

Screening projects – Include Alert Management Requirements

### Alert Management Workflow

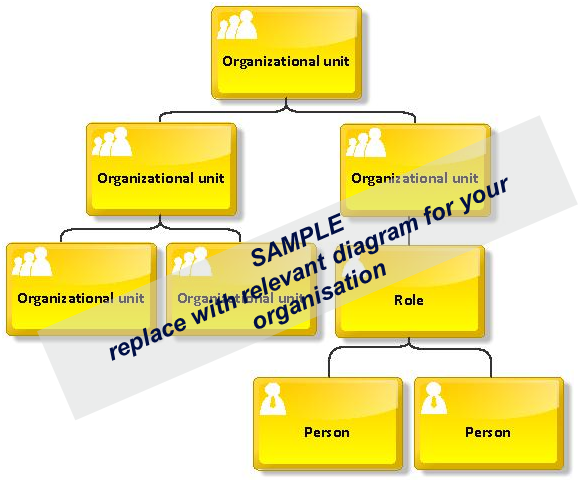


Figure 2 Future Organisation Structure Business Unit (n)

### Alert Management Requirements

Table — Alert Management Requirements

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
| BAL-001 | FAL-001 |  |
| ... | ... |  |
|  |  |  |
|  |  |  |

## Escalation Matrices

Screening projects Escalation Matrices requirements

### Escalation Matrices Representation

Screening projects – Add the Escalation Matrice graphic representation

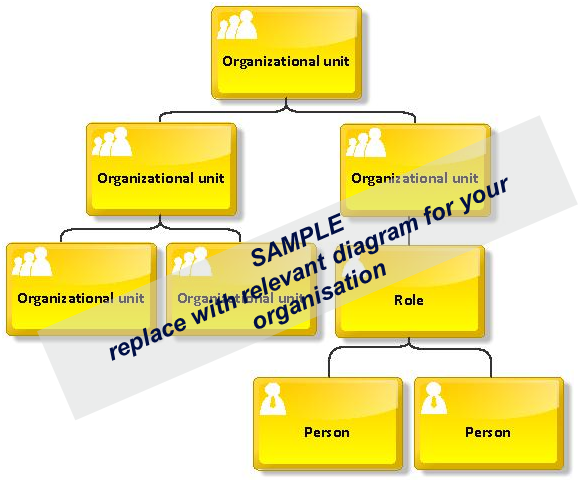


Figure 3 Future Organisation Structure Business Unit (n)

### Escalation Matrice Requirements

Table — Escalation Matrice Requirements

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
| BEL-001 | FES-001 |  |
| ... | ... |  |
|  |  |  |
|  |  |  |

## Controls Setup

Screening projects Include parameters in functional requirements if new or change include if control is defined at country/global, access to add/modify controls.

Table — Controls Setup

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
| BCO-001 | FCO-001 |  |
| ... | ... |  |
|  |  |  |
|  |  |  |

## Problem Management

Screening projects Problem Management requirements

Table — Problem Management

| BRD Ref | FSD Ref | Requirement |
| --- | --- | --- |
| BSP-001 | FSP-001 |  |
| ... | ... |  |
|  |  |  |
|  |  |  |

# Appendices

## Reference Material

(List all referenced documents here)

Table — Reference Material

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Document | Version | Location |
| [BLOCKS98] | Blocks J., *My life as a sample*, Acme Publishers, Acme City, 25 January 2003 |  | <include hyperlink> |

## Definitions and Acronyms

Provide definitions of special terms, acronyms referenced throughout the document

Table — Definitions and Acronyms

|  |  |
| --- | --- |
| Acronym/Abbreviation | Description |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Document History

Table 15—1 Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Summary of Changes | Author | Project Role |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Document Reviews

The Functional Specifications must be gathered from the project stakeholders and impacted functions and businesses and the related technology partners. Refer to TOR members and Stakeholder review.

Table 16—1 Document Reviews

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Reviewer Name | Reviewer Project Role | Reviewer | Approver |
| 2.0 | Tony Liang | Manager Credit Risk Management | Rebecca Chim | Tony Leung |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Document Approvals

Table 17—1 Document Approvals

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Approver Name | Approver Project Role | Approval |
|  |  |  | Accountable Executive |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Performance Goals

(Provide a further breakdown of performance goals based on requirements in Business Requirements Definition. E.g. Service Availability, Transaction Volume, Response Time)

# Application Overview

Describe the application to be built / functionality to be enhanced, how system functions address the requirements and list of systems to be interfaced. Also, describe in brief the major existing functionality.

Table — Existing Functionality

| # | Strategic Issue | Implications |
| --- | --- | --- |
|  |  |  |

Table — Intended changes

| # | Strategic Issue | Implications |
| --- | --- | --- |
|  |  |  |

Table — New/Changed Interfaces

| # | Strategic Issue | Implications |
| --- | --- | --- |
|  |  |  |