

## **Scope of the Project**

### **1.1 Introduction**

The portal will provide an integrated platform for the refinancing business/resource support business.

The key stakeholders of this platform are as below:

- Primary Lending Institutions (PLIs): These are financial institutions that provide financial assistance (loan) to the ultimate beneficiaries and have loan refinancing needs. The lenders can be present or unavailable on the lending marketplace platform. E.g.: Banks, FIs, NBFCs, MFIs, Fintechs, etc.
- Refinancing Institutions: Organization that provides refinancing option and financial assistance (loan) to the Primary Lending Institutions (in this case, SIDBI).

### **1.2 SIDBI's Expectations**

#### **1.2.1 Ecosystem**

1.2.1.1 The objective of this ecosystem is to provide refinance to various PLIs by enabling quick turnaround of process to provide refinance to the PLIs.

#### **1.2.2 Bidder**

The following is expected from the bidder

1.2.2.1 The Bidder shall Build and maintain the platform for a duration of 3 years with the option to extend for another 2 years and thereafter transfer the platform, IPR, data etc. to SIDBI

1.2.2.2 The Institutional Finance Vertical (IFV) already has a internal software in place which is utilized for processing. Bidder shall build a customized end-to-end platform on behalf of SIDBI

1.2.2.3 It must be ensured that existing software remains fully functional, uninterrupted and existing data, users and services together with the relationships are migrated to the new platform along with due hand holding to the users.

1.2.2.4 Provide knowledge transfer to relevant SIDBI personnel / any other external personnel appointed by SIDBI and annual maintenance facilities for the platform after transfer of the platform to SIDBI.

#### **1.2.3 Introduction**

The motive behind this platform is to build a tool which would enable Primary Lending Institutions (PLIs) to obtain refinancing from SIDBI for Micro and Small Loans in hassle-free manner. This platform is envisaged utilizing the latest in emerging technologies to enable quick and efficient refinancing processes.

SIDBI is looking for a comprehensive portal having the following capabilities:

- 1.2.3.1 **Single Platform for End-Users:** Common platform to manage end to end loan tracking and continuous communication between PLI and SIDBI.
- 1.2.3.2 **Single Customer View:** Portal should be able to provide a 360 view of a customer for a PLI and SIDBI including loan history, account information, etc. De-duplication to be performed before on-boarding any user.
- 1.2.3.3 **Integrated Eligibility Check:** Portal should be able to automate the process of determining the eligibility of the PLI for obtaining refinancing facility as well as the PLI's accounts for which refinancing is being requested.
- 1.2.3.4 **Auto-generation of Minimum Interest Rate and Processing Fees:** portal should be able to generate the minimum interest rate as well as the processing fees applicable for each individual lender based on Treasury Vertical inputs. **[this should be visible only to SIDBI]**
- 1.2.3.5 **Content Management:** Portal should be capable of storing large data / information including documents, etc.
- 1.2.3.6 **Historical Data:** Portal should be able to record historical data which is available anytime for reference for the authorized user. The data will be available for view based on user consent.
- 1.2.3.7 **Security Management:** Portal should be able highly secure in order to protect the sensitive data available. Portal should have antivirus feature and anti-hacking feature.
- 1.2.3.8 **Helpdesk Management:** Portal should facilitate quicker grievance resolution and facilitate feedback from users.

#### **1.2.4 Key Feature**

The platform is envisioned as having the following features:

- 1.2.4.1 **Primary Lending Institution (PLI) Registration:** PLI will have registration process which will be simple, easily understandable and self-explanatory. Registration requirements for each segment of PLI shall be built into the portal to capture all relevant data for eligibility checking. While registering, there should be a pull-down menu, giving the various entities viz banks, small finance banks, NBFCs, MFIs and Fintech, etc.
- 1.2.4.2 **Document and Content Management:** Based upon the entity upon which the registration is proposed the product or scheme should be displayed, out of which PLI can choose to apply. Platform will have capability to store the documents like, but not limited to, financial statements, beneficiary list, CS certificates, Quarterly Monitoring Reports, etc. in bulk with focus on digital content. User will be allowed to access, view

documents, individual feedback, download applicable formats, etc. There should be a maker/checker concept at the level of PLI while submitting any information.

- 1.2.4.3 Loan Processing: Portal to enable Refinancing Institution users to conduct loan processing from the portal itself including checking eligibility for PLI and ultimate beneficiary, processing of loan, providing interest rates, determining amount of processing fees applicable, exposure checking, policy checking, etc. This will entail integration of platform with systems of other functions as applicable.

Further, there will be a pull-down menu for selection of scheme under which the application is being submitted, so that proper documents may appear for submission and portal should have the provision that the application can be under more than one scheme at a time [for example, MSERS and RMSE]

There should be a provision for checking the various due diligence sites viz CIBIL, wilful defaulters, RBI fraud, CRILIC, etc

- 1.2.4.4 Reviews, Ratings and Feedback: The PLI and Refinancing Institution will have an option of providing reviews and feedback on the portal and rate each other on the basis of quality of service, interactions, etc., for the whole loan lifecycle. The portal shall have a rating engine that would rate the PLI on the basis of a number of parameters including feedback, loan repayment time etc. Visibility of ratings shall be determined through configurable business rules.
- 1.2.4.5 Data analytics and business intelligence: The platform will provide comprehensive monitoring through Business Intelligence (Dashboards and reports) and will provide strong analytics capability. The mechanism would also allow for alerts, reminders, etc. to be sent through a unified dashboard that will keep lenders informed. Bidder should provide functionality to generate 20 reports in an automated fashion. The exact formats of the reports will be communicated during implementation of portal. In addition, the portal should allow design of customised reports as and when required.
- 1.2.4.6 Fraud and cyber security: The platform will provide enhanced security services for fraud mitigation and provide best technologies to protect from unauthorized access and fraud content.

## **1.2.5 Business Flows**

- 1.2.5.1 The workflow will cater to the PLIs who approach the Refinancing institution for refinancing. Please refer to Annexure A for details on workflows.
- 1.2.5.2 The PLI, in its own capacity, will provide all the data and documents that are needed for the refinancing. PLI and the Refinancing institution will directly interact with each other through the portal.

## **1.2.6 Business Architecture**

1.2.6.1 The portal will include following modules as part of the platform but not limited to:

- Product management: Robust platform to handle various stages of product management such as
  - a. Sourcing of applications
  - b. Loan processing
  - c. Credit appraisal, monitoring and tracking
- PLI management: Platform should have capability for quick registration & on-boarding of PLI. Platform should be able to perform categorization of PLI based on certain parameters.
- Service management: Platform should have capability for configuration of dashboards for various user types
- Catalogue & Content management: Portal should have the capability to record and store the loan history and store documents for future reference
- Loan Lifecycle Management: Portal should have the capability to handle end to end loan lifecycle including relevant features required for monitoring.
- Credit underwriting and scoring: Portal should provide credit scoring capabilities for each of the PLI depending upon the data provided by the Central Information Commission, rating agencies/ credit bureaus, data providers and internal scoring model of Refinancing Institution wherever available
- Monitoring: There should be a provision for uploading the visit reports and photographs from offsite
- Analytics: Platform should have provision to perform analytics such as performance analytics and business analytics on the data available on PLI and provide easily understandable output for decision making and understand PLI better
- Operational data store: Platform should have feature to generate reports, dashboards which shall be available on real time basis to the users. Bidder to provide report generation features for up to 20 adhoc reports as prescribed by SIDBI.
- Customer grievances: Platform should allow users to log queries and grievances through portal or call. This portal should be used to manage all PLI interactions and also act as a repository to be used for analysis of feedback & grievances. The portal should be capable of taking caller satisfaction feedback on email, portal or call.

- 1.2.6.2 Customized dashboard will be provided for each PLI which will have the view of the loan applications, loan statuses, etc.
- 1.2.6.3 The platform should have OCR to technology inbuilt to receive meaningful information from images.
- 1.2.6.4 Bidders are required to refer to the RBI Master Circular DBOD No. Rajbhasha.BC. 25/06.11.04/2012-13 dated: 29/09/2017 July 2, 2012 on the 'Use of Hindi in Banks'. The Master Circular has been suitable updated by incorporating instructions issued up to June 30, 2013 and hosted placed on the RBI website (<http://www.rbi.org.in>) i.e. the platform should be available at least in Hindi and English.
- 1.2.6.5 The platform should have in-built safeguards and security features to protect itself from the external threats and interruptions. There should be failover mechanism available within the portal.
- 1.2.6.6 The platform shall have the capability to support 200 Queries Per Second and a response time of 500 ms. It should be scalable to meet the requirements of SLAs.
- 1.2.6.7 To ensure full availability of the application during working hours, alternative facilities should be provided in case exception in live environment.
- 1.2.6.8 A single view of the customer experience and history. The portal shall be designed to give a single view of all interactions.

## **1.2.7 Business Modules**

### **1.2.7.1 PLI Management**

This section details the services to be provided for PLI's management. The PLI's management shall include but not limited to the following stages:

- **Qualification & Registration**

The Bidder shall define the qualification and verification criteria on the platform in consultation with Refinancing Institution and any PLI should get on-boarded only with approval from Refinancing Institution. The Bidder shall create the provision for online PLI registration of the PLI through secure login mechanism. Any new PLI should be able to apply for registration on the PLI registration panel. Based on the qualification and verification agreed criteria, platform shall communicate the acceptance or rejection of the PLI. All rejection cases must be accompanied by the reason for rejection.

- **On-boarding Manual**

The Bidder shall create an on-boarding manual for the PLI registration and lifecycle management of the PLI on platform. The Bidder shall continuously update the on-boarding manual.

- Support for PLI

The Bidder shall offer assistance to PLI for redressal of the grievance by issuing a ticket and resolution of the ticket in a time bound manner.

- Communication

The new registration is to be communicated to the PLI through e-mail.

- PLI Rating

The Bidder shall define a process for feedback and rating of the PLI on platform.

- PLI Exit Management

SIDBI shall manage exit / termination of PLI on the platform. Bidder needs to give adequate functionalities accordingly.

- Deliverable

Under this category, the Bidder shall specifically deliver the following but not limited to

a. Development, Implementation and enhancement of platform's PLI Interface Portal

b. Detailed Help-Manual for On-boarding of PLI covering the entire Scope of Work as mentioned in above section.

i. A draft Business Architecture.

ii. While preparing the Manual for on-boarding the bidder is expected to adapt the Business Processes so created and update them if required to create the Manual for on-boarding the PLI for complying to the Scope of Work as mentioned above.

c. Preparation of draft PLI's Agreement for on-boarding of PLI.

#### 1.2.7.2 Product Management

The bidder is responsible for Product management and bidder shall ensure that the portal takes care of as many stages of lending lifecycle as per the Business Processes. The Product Management shall include but not limited to the following stages:

- Lending Request by PLI

The bidder shall provision a dashboard for the registered PLIs for making a loan request and Refinancing Institution to view the loan request on the dashboard depending upon the rules predefined.

- Modifying Loan Request

The bidder shall ensure that the PLI is able to modify the loan request only till the submission of the application. Subsequently, SIDBI shall have the right to accept / reject / return the application to the PLI.

- Archiving Loan Request

The bidder shall ensure that the loans with statuses as, but not limited to, rejected, completed should be automatically be archived post predefined period.

- Post Disbursal Request

Post disbursement, the PLI should be able to make certain requests i.e., for issuance of NOC, Paripassu charge, satisfaction of charge, prepayment request, reduction in interest rate, etc.

## **1.2.8 Technical Design Considerations**

The platform should be built keeping in mind the following considerations:

### **1.2.8.1 Continuous adoption of rapidly evolving Technology**

The platform should be open (standards, open API, plug-n-play capabilities), components coupled loosely to allow changes in sub-system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment. The platform should be robust enough to handle continuous changes.

### **1.2.8.2 Provision of a Sustainable, Scalable solution**

The motive of this platform is to provide a portal that would be sustainable for the next few years. The expectation is that the portal should sustain at least 10 years from Go-Live. The platform should be created keeping in mind the scalability of the portal. The simplified lending processes and ease of compliance is expected to lead to huge growth in contract's base. Every component of the platform needs to scale horizontally to very large volume of data. The platform should be built to be scalable for up to 300 PLIs.

### **1.2.8.3 Distributed access and Multi-channel service delivery**

With high penetration of mobile devices and very large percentage of internet usage using mobile devices, it is imperative that portal should provide multiple channels of service delivery to constituents. An important consideration is that the access devices and their screen capabilities (including browser variations) are numerous and constantly evolve. One of the design considerations is to provide seamless interfaces over laptop/tablet and mobile devices to PLIs to interact with the platform.

### **1.2.8.4 API approach**

The aim of the project is to reuse the already built in API components which are available free with GOI and which are applicable for refinancing business keeping in mind aspects such as security, authenticity, continuity, etc.

### **1.2.8.5 Security & Privacy**

Security and privacy of data should be fundamental in design of the portal without sacrificing utility of the portal. When creating a portal of this scale, it is imperative

that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the portal from day one.

#### 1.2.8.6 Business Rule Driven Approach

All configurations including policy decisions, business parameters, rules, etc. shall be captured in a central place within the portal. The portal shall provide facility to the administrator to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Managing these in a central repository ensures only one source of truth is used across many application servers and reduces issues of inconsistent application behaviour.

Decoupling of the business parameters/rules/master data from the rest of the portal architecture and making them configurable allows for a great deal of flexibility. There should be a central interface for managing the configurability by authorized user group

#### 1.2.8.7 SLA driven Approach

Portal should be available 24\*7 covering all the business functionalities. Downtime should be responded based on the criticality of the issue, below factors to be considered on response:

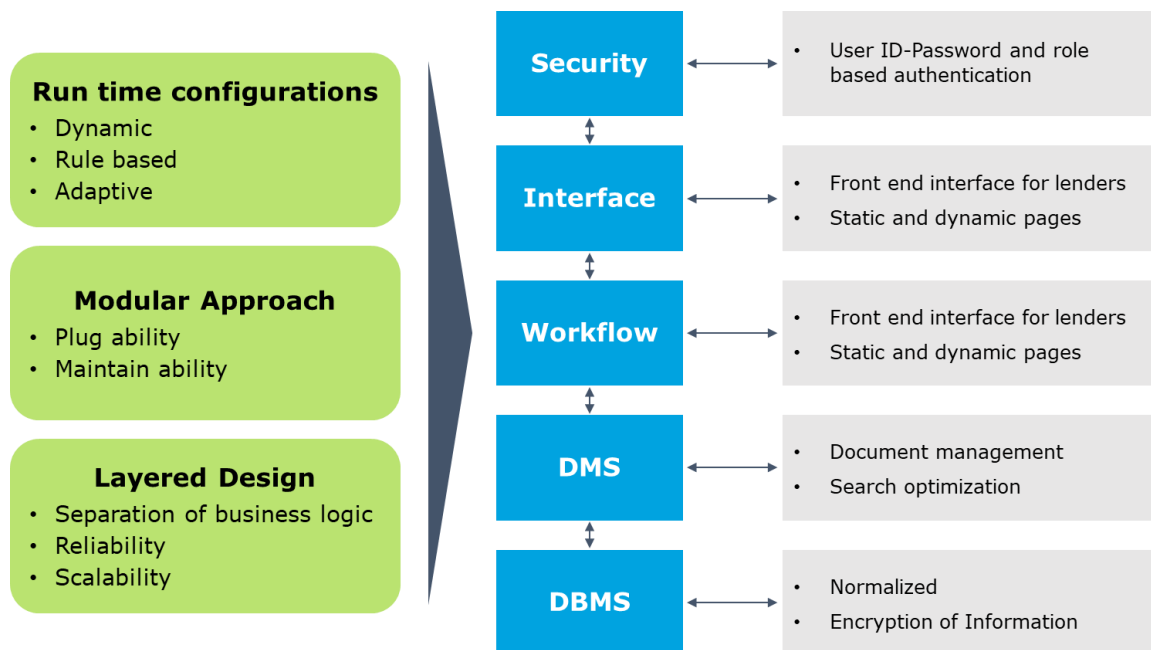
- Maximum time that can be taken to acknowledge the reported problem
- Maximum time that can be taken to fix the problem & release the same into production.

### **1.2.9 Technical - Guiding Architectural Principles**

The IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks and future state target architecture.

The overall portal will be build based of the following indicative architectural principles which will be the backbone of the overall portal architecture:





**Fig. xxx - Illustrative Architecture principles**

The platform will need to be built on the following core principles:

#### 1.2.9.1 Platform Approach

Open APIs designed to be used to ensure openness, multiuser ecosystem, specific vendor/system independence, and most importantly providing players with choice of using innovative applications on various devices (mobile, tablet, etc.) that are built on top of these APIs.

#### 1.2.9.2 Performance

A best of breed portal using the leading technologies of the domain should be proposed in the portal ensuring the highest levels of performance. It will also ensure that the performance of various modules should be independent of each other to enhance the overall performance and also in case of disaster, performance of one module should not impact the performance other modules.

The portal should be designed in a manner that the following can be achieved:

- Modular design to distribute the appropriate system functions on web and app server
- Increase in-memory Operations (use static operations)
- Reduce number of I/O operations and N/w calls using selective caching
- Dedicated schemas for each function making them independent and avoiding delays due to other function accessing the same schema

#### 1.2.9.3 Scalability

The component in the architecture will be capable of being scaled up to, cater to, large number of loan requests. Even inclusion of additional application

functionalities can be catered to by upgrading the software editions with minimal effort.

The design of the portal to consider future proofing the systems for volume handling requirements

- The application functions to be divided logically and developed as Modular solution
- The portal should be able to scale horizontally & vertically
- Data Volume – Ability to support at least 500% projected volume growth, post portal implementation at any time
- Functionality – Ability to extend functionality of the solution without significant impact to the existing functional components and infrastructure

#### 1.2.9.4 Security

The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to.

The portal should be designed to provide the appropriate security levels commiserate with the domain of operation. Also the portal will ensure data confidentiality and data integrity.

The application system should have the following

- Data security policies and standards to be developed and adopted
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements
- Role based access for all the stakeholders envisaged to access and use the portal
- Appropriate authentication mechanism adhering to industry good practice of Password Policies etc.
- Ability to adopt other authentication mechanism such as Electronic Signature Certificates
- Authorization validity to be ensured for the users providing the Data to the portal. Data should be accepted only from the entity authorized
- Data should be visible only to the authorized entity
- Audit trails and Audit logging mechanism to be built in the portal to ensure that user action can be established and can be investigated if any can be aided (E.g. Logging of IP Address etc.)

- Data alterations etc. through unauthorized channel should be prevented
- Industry good practice for coding of application so as to ensure sustenance to the Application Vulnerability Assessment

The infrastructure security should cover the following:

- Security log monitoring services
- Anti-Phishing Services including identification and mitigation of attacks
- Malware and Trojan scanning, monitoring, mitigation services
- Security Dashboard, Threat monitoring & Analysis
- Security Analysis, Mitigation and prompt reporting thereof

#### 1.2.9.5 Reliability

This is a very crucial system and data is of high sensitivity, the data transfer and data management should be reliable to keep the confidence of the stakeholders. The portal should have appropriate measures to ensure processing reliability for the data received or accessed through the application.

It may be necessary to mainly ensure the following

- Prevent processing of duplicate incoming files /data
- Unauthorized alteration to the Data uploaded to the platform should be prevented
- Ensure no data loss

#### 1.2.9.6 Manageability

It is essential that the application architecture handles different failures properly; be it a hardware failure, network outage, or software crashes. The portal must be resilient to failures and have the ability to restart and make human intervention minimal. All layers of the portal such as application, infrastructure must be managed through automation and proactive alerting rather than using multiple people manually managing.

#### 1.2.9.7 Availability

The portal design and deployment architecture will ensure that the application can be deployed in a centralized environment offering portal high availability and failover.

The portal should meet the following availability requirements

- Portal should be hosted on SIDBI's servers
- Load Balanced across two or more Web Server avoiding single point of failure
- Deployment of multiple application instances should be possible

- Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance

#### 1.2.9.8 Reconstruction of truth

Portal should not allow database /system administrators to make any changes to data. It should ensure that the data and file (data at rest) that is kept in the systems has tamper resistance capacity and source of truth (original data of invoices and final returns) could be used to reconstruct derived data such as ledgers and system generated returns. Portal should be able to detect any data tampering through matching of hash value and should be able to reconstruct the truth.

### **1.2.10 Technical Architecture**

Technical architecture of the envisaged platform includes layer wise different business services, external integration, content management, MIS reporting, workflow implementation, and notification services

The logical layers identified for the proposed architecture are as follows:

- Client Layer
- Presentation Layer
- Business Layer
- Data Storage Layer
- Data Analytics Layer
- Integration Layer

#### 1.2.10.1 Client Layer

This layer represents the users or stakeholders who will be using the portal for on boarding, loan request, viewing reports/dashboards, monitoring loan application, submitting/ uploading document etc. Besides the front-end users there will be back-end users who will be acting on the service request raised, verify and approve or reject application accordingly.

All access to the portal will be either through intranet leveraging the LAN/WAN connectivity or over the internet through broadband/3G/4G connectivity or over the mobile/smart phones through cellular (GSM) network. A specific user can have only one access instance from the mobile channel and one instance on the web channel of the portal at a particular time.

#### 1.2.10.2 Presentation Layer

The presentation layer is catered for the platform, it encapsulates all presentation logics required to service the users that access the portal. This layer intercepts all client http requests, authenticates the users, conducts session management, controls access to business services, constructs the response and delivers the http response back to the client

This layer will cater to the following key services

- MVC Framework Service

Based on static and dynamic requirements of the presentation services, there can be the client side and server-side components in this layer.

- a. Client Components: These are static components required for rendering the UI pages and include HTML, Java scripts, style sheets, image, icons etc.
- b. Server Component: These are the dynamic components that are required for processing of client request. Popular MVC framework can be used and leverage the framework's rich tag libraries and MVC (Model-View-Controller) capability.

- Portal Services

Every user needs to pass through strong authentication before serving with personal 'Dashboard' as home page, the contents of which are dynamically decided based on the accesses permitted to the users. In no case, a user shall be allowed multiple logins from any device(s).

The generation / reset of password should be automated. In case of locking of password or change of password, the portal should ask for certain credentials based on the correctness of which, the password should be auto-generated, and the reset password should go by way of a mail to the registered mail id [common mail id] of the PLI

Some of the specifications of the web portal are provided below:

- a. UI layer should not have its data
- b. The portal should not allow concurrent sessions for same user. The portal should automatically log out a customer in case of session breakdowns (e.g., communication failure, high inactivity period - these should be parameterized)
- c. The portal should support workflows
- d. The portal should implement security features, such as password complexity, automatic blocking (temporary/permanent) of user logins after given number of unsuccessful login attempts (should be parameterized), controlled access to content stored on the portal and logging of security incidents. It should be by its own or through an integrated Identity Management solution and should be capable of managing security rights and privileges by individual, group and role.
- e. Portal should support HTTPS protocol on Secure Socket Layer (SSL).
- f. The portal should support the leading browsers such as Internet Explorer, Firefox, and Chrome etc.

- g. The portal should be able to expose /publish functional applications seamlessly
- h. The portal should provide search engine with advanced full-text search capabilities based on the user. The search engine should be able to search for requests within the portal.
- i. Should provide support for comprehensive audit trail features such as:
  - i. Daily activities log should be merged into the history log files
  - ii. All screens should display system information
  - iii. Daily activity reports should be provided to highlight all the applications being processed during the day
  - iv. Unsuccessful attempts to log-in to the portal should be recorded
- j. Portal should be compatible to popular mobile devices Operating systems
- k. Portal should be interoperable with industry standard databases
- l. In addition, the portal should provide the following capabilities
  - i. Should be able to integrate with common office application
  - ii. Should authenticate users from Active Directory/LDAP, claim based authentication
  - iii. Should support virtualization
  - iv. Should support customization of look and feel of the portal
  - v. Should support a broad range of standards, preferably open standards. Some examples are DOM 1.0, HTML 5, HTTP, HTTPS, Math ML, ODBC , ODF (IS26300), Open XML (IS29500), Open Search, Open Type, PDF 1.7, PDF/A, RTF, RSS, ATOM, SOAP, SVG, REST, UDDI, Unicode, URI/URN, W3C XML Schema, WCAG 2.0, Web DAV, WSDL, WSRP, XHTML, XML, XML Web Services, XML Dsig, XPATH, XPS, XSLT
- m. Should integrate with standard email services
- n. Should integrate with any other portal products through open standards such as HTML, XML, RSS, web services, and WSRP
- o. Should support encryption and compression features
- p. Should support multiple roles with associated access controls

- q. Should support upload, store, organize and share documents
- r. Should provide multi-channel output capabilities
- s. Users should be able to upload documents in specified formats
- t. Users should be able to upload multiple files at the same time
- u. Should support version control, change tracking and comments in these documents
  - i. Should support document linking capabilities (static, dynamic, and/or other)
  - ii. Should support the import of content into the repository
  - iii. Should support document and text indexing capabilities
  - iv. Should support image indexing capabilities
  - v. Should be able to support to store and manage documents in the same repository
  - vi. Should Support Managed Metadata
  - vii. Should support content archiving capabilities
  - viii. Should provide offline support for forms
  - ix. Should support creation of ad hoc query by users
  - x. Upload document will be in Word, XML, CSV and excel. Scanned document will be in PDF and images in JPEG, PNG
  - xi. While uploading bulk data it should also tell for errors if it encounters any. The data formats for the list of beneficiaries should be fixed and there should be an option to download the blank format, fill in the details and upload the same. No changes in the format should be allowed

- Security Services

The security service will provide the following security control features –

- a. User Registration & User Profile Management

System Administrators can administer the application security through a web interface that will allow them to register and create user profiles for users who will access the platform. User Registration service will allow administrators to perform activities like registration and login features, creation/editing/deletion of user profiles and groups, assigning roles to users, assigning users to groups etc.

User Profile Management Service describes how to customize the self-registration process for creating user accounts, and how users edit their account profiles in the platform.

There should be alert for the users to one stage higher authority for information and necessary action based on escalation matrix

b. User Authentication

Highly configurable web security services provided by the HTTP Server like Apache will be leveraged, which adds a comprehensive set of Web single sign-on services and extends them further with centralized user provisioning that is available in any open LDAP, version 3-compliant directory service. End users logging on to the portal will be authenticated against the user name /password credentials and all documents will be authenticated against Digital Signature/ e-Sign.

In addition, the application server's underlying authentication provider services for enterprise application security to authenticate user identity can be utilized. Refer to the security architecture section below in this document.

c. User Authorization

Users, groups, roles and security policies will be defined to prevent unauthorized access to specific platform services. The application server's underlying authorization provider service can be availed to authorize user access.

- Business Presentation (UI) Services

The UI interface should be interactive and user friendly.

- Caching Services

The caching services can be static, dynamic as well as distributed.

- User Personalization & Dashboard Services

Portal should provide user personalization services allowing users to maintain their own specific profiles. Each user will be presented with a centralized dashboard view specific to each user profile that will display key information in a summarized manner.

- Report UI Services

This service will present the user interface to the end users to provide reporting criteria, complex querying and view MIS/Custom/Analytics reports generated by the business layer MIS and Analytics reporting components.

- Calendar Services



This custom service will provide the Calendar functionality in the UM2 application. This component will be custom built leveraging the MVC framework components. The service will display the date and time of all events scheduled in a standard monthly calendar format.

### 1.2.10.3 Business Layer

The business layer will manage the IFV business services for its stakeholders. All business processing for the application will be centralized in this layer. It receives requests from the presentation tier, processes the business logic based on the requests, and mediates access to the other underlying layer (data access/storage layer or integration layer) resources. Additionally, this layer will handle content management services, database connection management, session management, email notifications, interfacing with payment gateway, integration with other applications and third party solutions

The following services will be provided by the business layer:

- Business Services & Service Request Common Components

These are the platform business layer components that will provide the business logic and rules to achieve the desired functionality. It will handle the requests coming from the presentation layer business presentation services and process the business logic based on the request. These services can in turn call common service components, workflow process engines, notification service or content services based on the type of processing requested by the presentation layer. It mediates access to the data access and storage layer to retrieve data from the data store or persist data in the data store.

- Notification & Messaging Services

The Notification Services will let the platform users perform simple email functions, such as view, create and delete messages, automatically create messages as part of the business flow with attachments and reply to or forward an existing mail. It simply enables users to use mail, manually or automatically, in a single collaborative environment. The Notification Services expose data from an existing mail server based on IMAP4 and SMTP protocol.

Notification Services also include services which will send emails alerts and notifications to the respective/relative PLI based on specific business process event that occurs during the service request life cycle. The flexible architecture of Notification Services will eliminate the pains of implementing features such as polling events, scheduling, formatting and delivery of notifications

- Analytics Reporting Services

Use of Analytics Reporting Services has been considered to be the most important aspect of the platform, in terms of getting intelligent insights out of the streaming data received real-time from the smart devices and social

media apps. SIDBI will be able to generate the Analytics Reports at various levels to perform predictive analysis, operational analysis, risk modelling, statistical analysis and monetization analysis for taking informed decisions. The proposed portal architecture will make use of the open standards framework compatible with the technology. The Reporting tool should have robust visualizations such as graphs, charts, and histograms.

The reporting tool should have slicing and dicing features facilitating ad-hoc management reporting on the fly. The reporting tool should have basic statistical modelling properties, so that SIDBI can create clusters, conduct regression analysis, and other modelling techniques dynamically.

The reporting tool should output data in various formats.

DBAs and end users to use a web-based portal to evaluate and understand the state of their system.

This feature should be available only to SIDBI users

- Support Services

These services will provide support functionalities like audit trail, error & exception handling, logging, export & printing services to the business components of the platform.

- a. Audit Trail Services: There is a design need to verify that transactions in platform are being processed correctly and honestly. Audit Trail Services will maintain a historical record of transactions that have been applied to an object or set of objects. General Information and Submission of RFP Response
- b. Exception, error handling & logging services: A robust and reliable application error handling mechanism should be part of the basic infrastructure which will handle normal situation as well as unexpected application error. Error detection, error handling, propagation of error information and error logging capabilities will be considered to make the application robust.

#### 1.2.10.4 Data Storage Layer

This layer is responsible for communicating with external source system and data stores. All access to the underlying platform databases will be through this layer. Typically, the business layer is coupled with the data storage layer whenever the business services requires data or services that resides in the Data Storage layer. All platform data access objects will reside in this layer and use JDBC technology to connect to the databases. An Object Relationship Mapping (ORM) framework steps in to fill this gap providing an easy to use and powerful object-relational persistence framework. The ORM Data Access Services will provide persistence to the platform data in enterprise database and facilitate creation, update and deletion of entities and relations. All the persistent records like business transaction details, workflow information, user information, emails are stored in this persistence layer in different format. Transaction details and workflow

information would be stored in DBMS while emails are stored in email server. User information would be stored in Directory server for faster authentication. The application framework will authenticate the users against active directory server.

Suggested specification of the proposed DBMS is mentioned below:

- All the applications implemented should have provision for optimizing the number of static connections to the database using connection pooling. All the applications implemented should also optimize the duration of connection to the database by using techniques like session time out
- It should support User-defined Data Types & User-defined Functions
- Database should support advanced data compression, self-healing and deployment in various cluster topology.
- The database platform should support enhanced configuration and management of audits
- The database platform should support Failover Clustering and disaster recovery solutions
- Database should support Schemas, Roles Based Privileges & Authentication
- The database should have enterprise level DB- support centre with helpdesk support
- Database security should provide different layers of database users with overall control of database security administrator, only authorized database administration users with assigned privilege should be allowed to access database
- A separate audit trail should be maintained for any direct modification, deletion and addition in DBMS database in database structure or records

#### 1.2.10.5 Data Analytics Layer

This layer is responsible for receiving the structured, semi-structured and unstructured data from the different data stores and performing the data mining and analytics of the same for generating useful business insights that can be used by various stakeholders to take informed decisions. There will be two separate data analytics engine, one for the business intelligence and dashboard of traditional enterprise data warehouse and the other for applying intelligent algorithms and analytics to interpret and provide utility to the aggregated unstructured data and getting outputs of tangible values, insights or recommendations.

- The data-warehousing platform should have capability to perform daily incremental load
- The infrastructure should have data quality and data profiling capacities
- The tool should be capable to handle extraction, transformation and loading of both structured and unstructured data from various data sources

- The data-warehousing landscape should be capable to handle huge volumes of data
- The portal should create a single source of truth by integrating disparate data from multiple sources and use that for analysis
- Proposed portal should have capabilities for online analytical processing
- The proposed portal should be capable of search-based data discovery
- Portal should have an in-built Backup, Archive, and Restore solution to protect data and ensure availability after Portal hardware failures, Application failure or corruption, Data corruption or loss, user errors or Disasters

#### 1.2.10.6 Integration Layer

All interfacing with external systems and internal application will take place through this layer. External systems will not have direct access to the platform database, but instead will be calling the relevant business services in the business layer for availing the information.

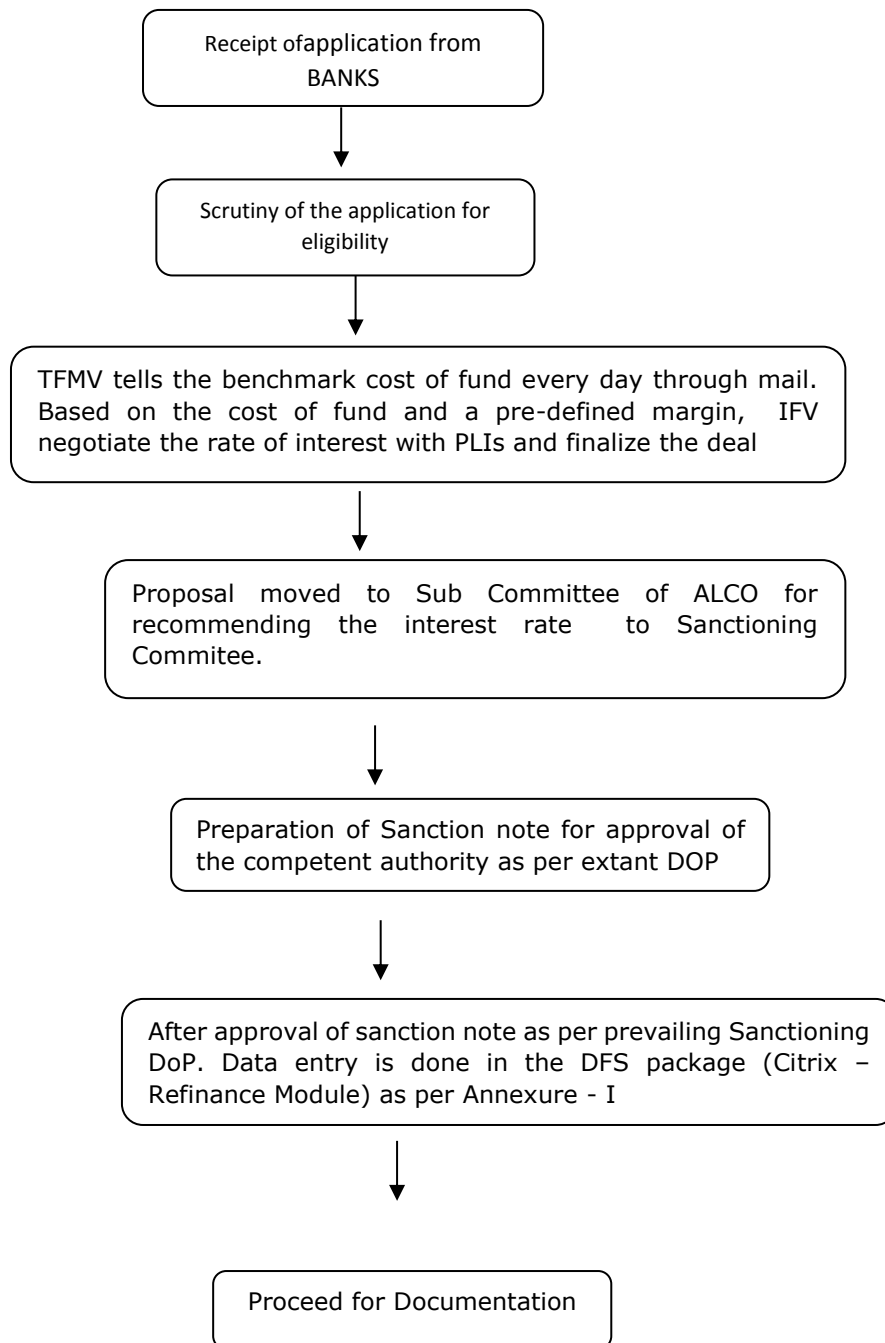
### **1.3 Success Factors**

The success of the platform will depend on the following factors, but not limited to

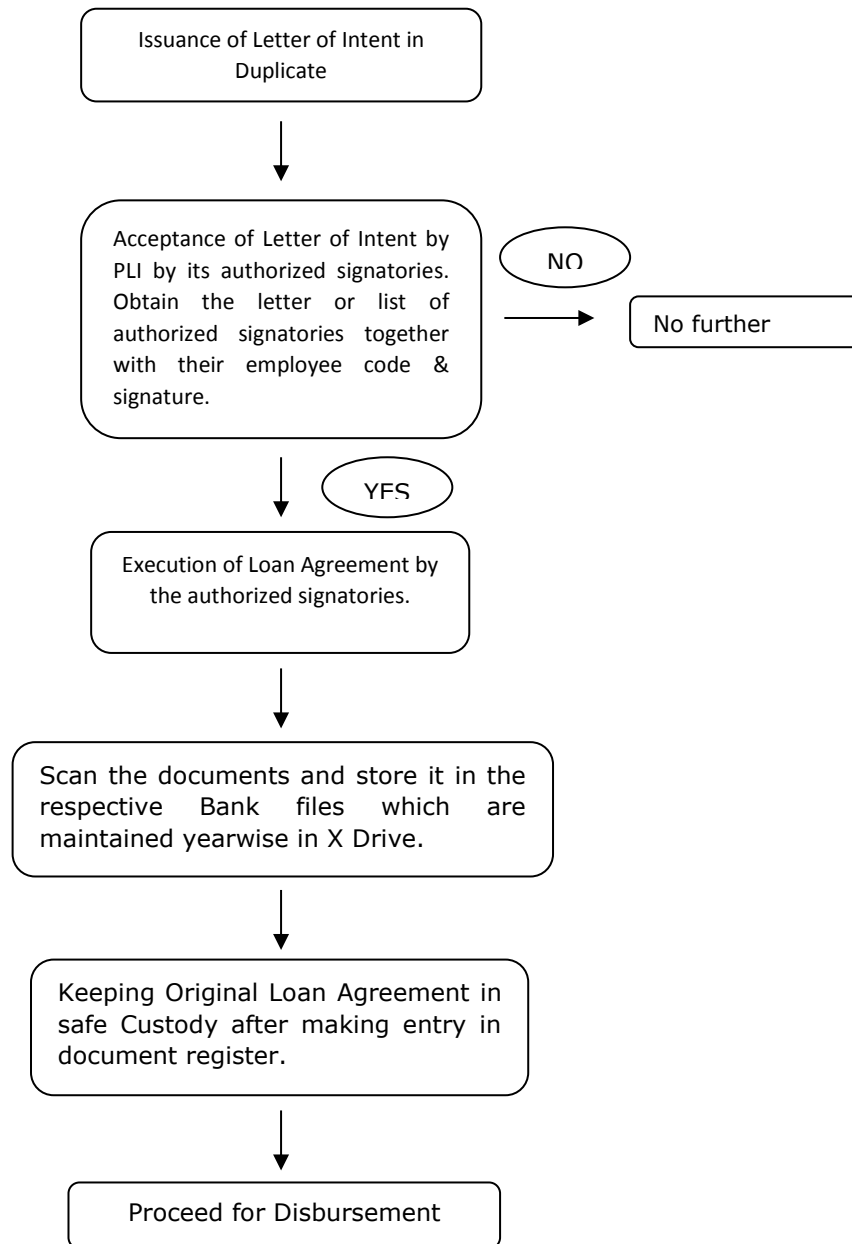
- 1.3.1 Business Scale: This parameter will be dependent upon the increase in number of active PLIs, number of refinancing requests & fulfilment and amount of refinancing disbursed to the borrowers.
- 1.3.2 Flexibility: This parameter will be based on whether portal is able to accommodate newer sources of data and alignment of business rules with the expectations of PLI.

## Annexure A - Workflows

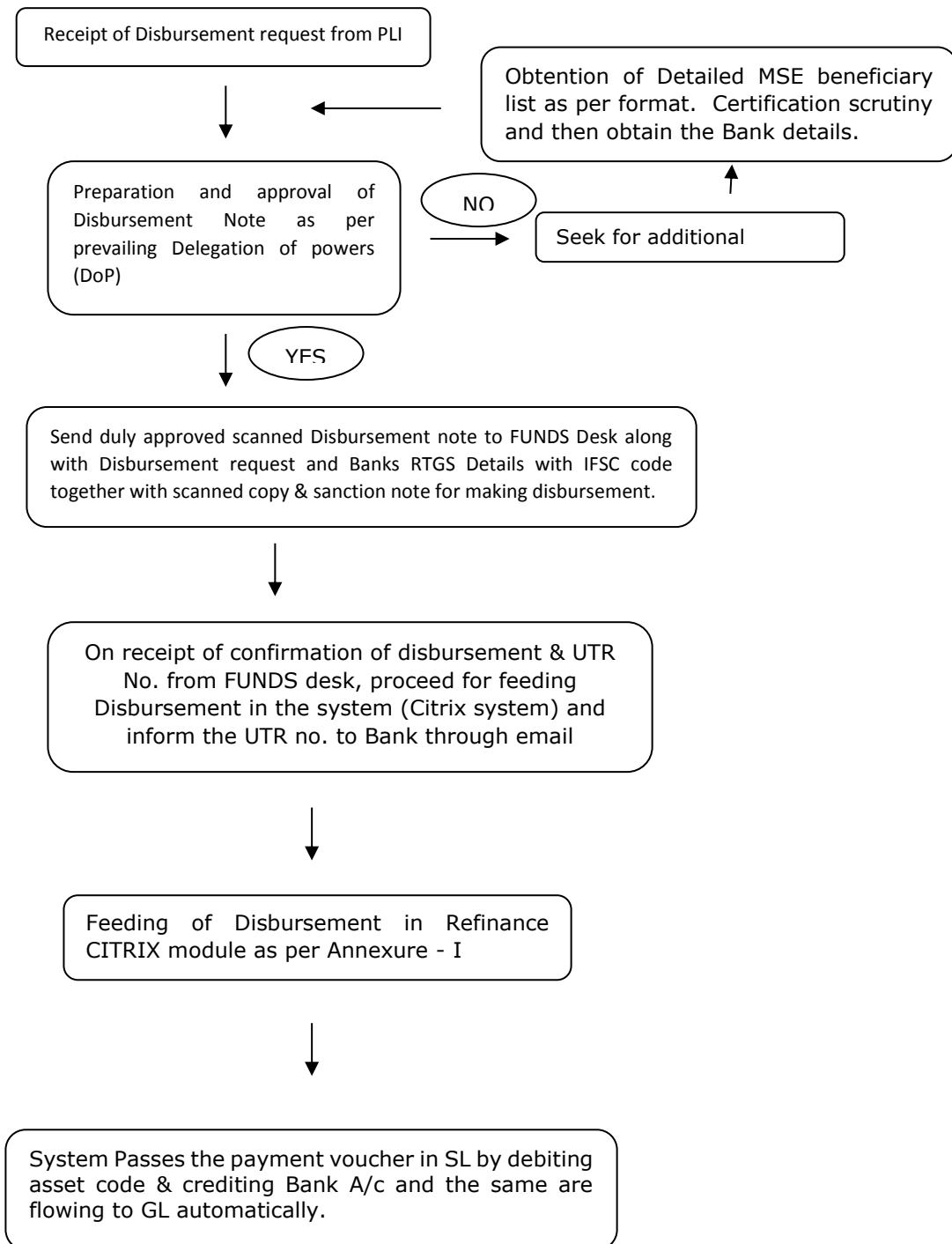
### **i. Refinance to BANKS - Sanction Process**



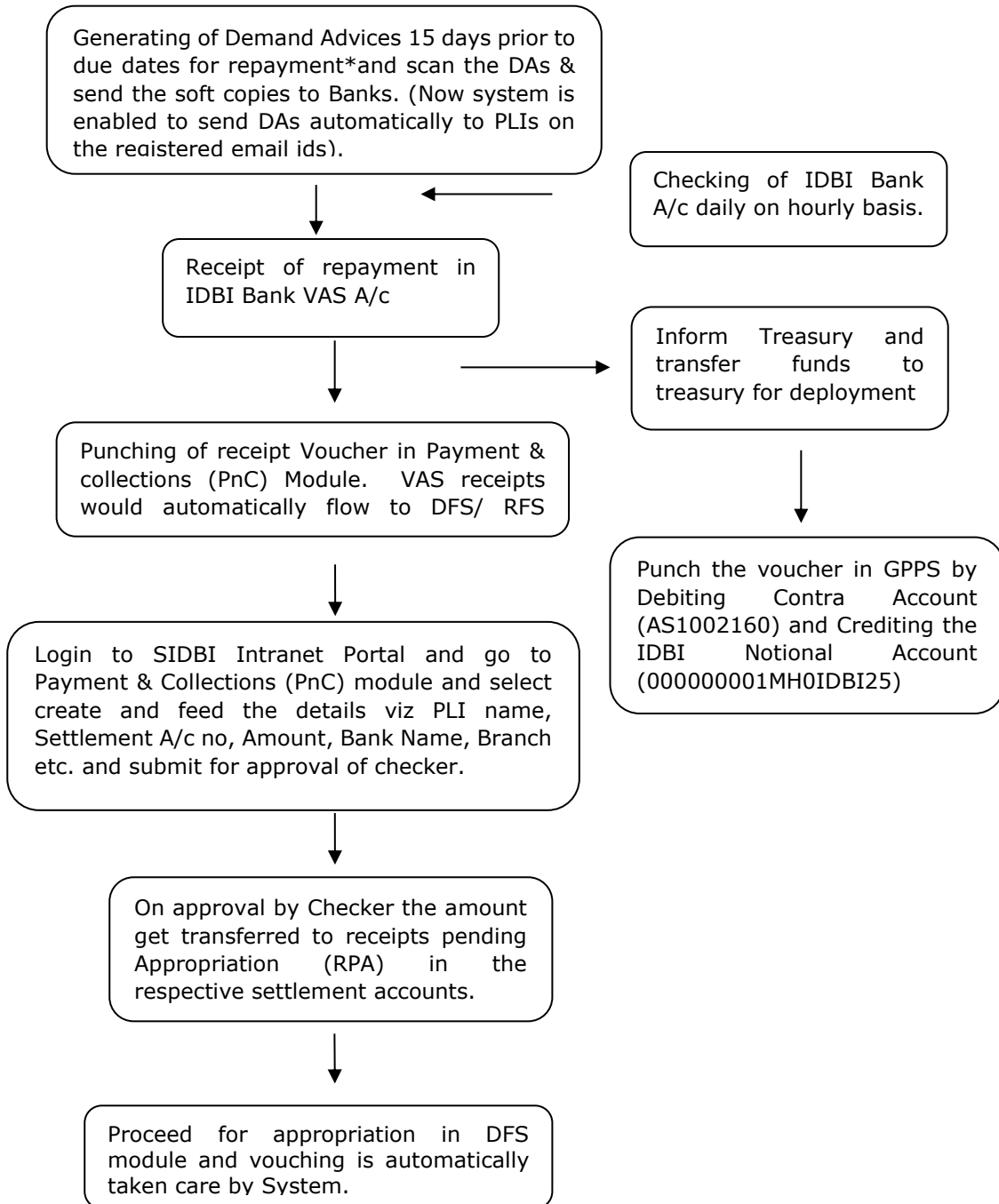
ii. **Refinance to BANKS– Documentation**



### iii. Refinance to BANKS– Disbursement

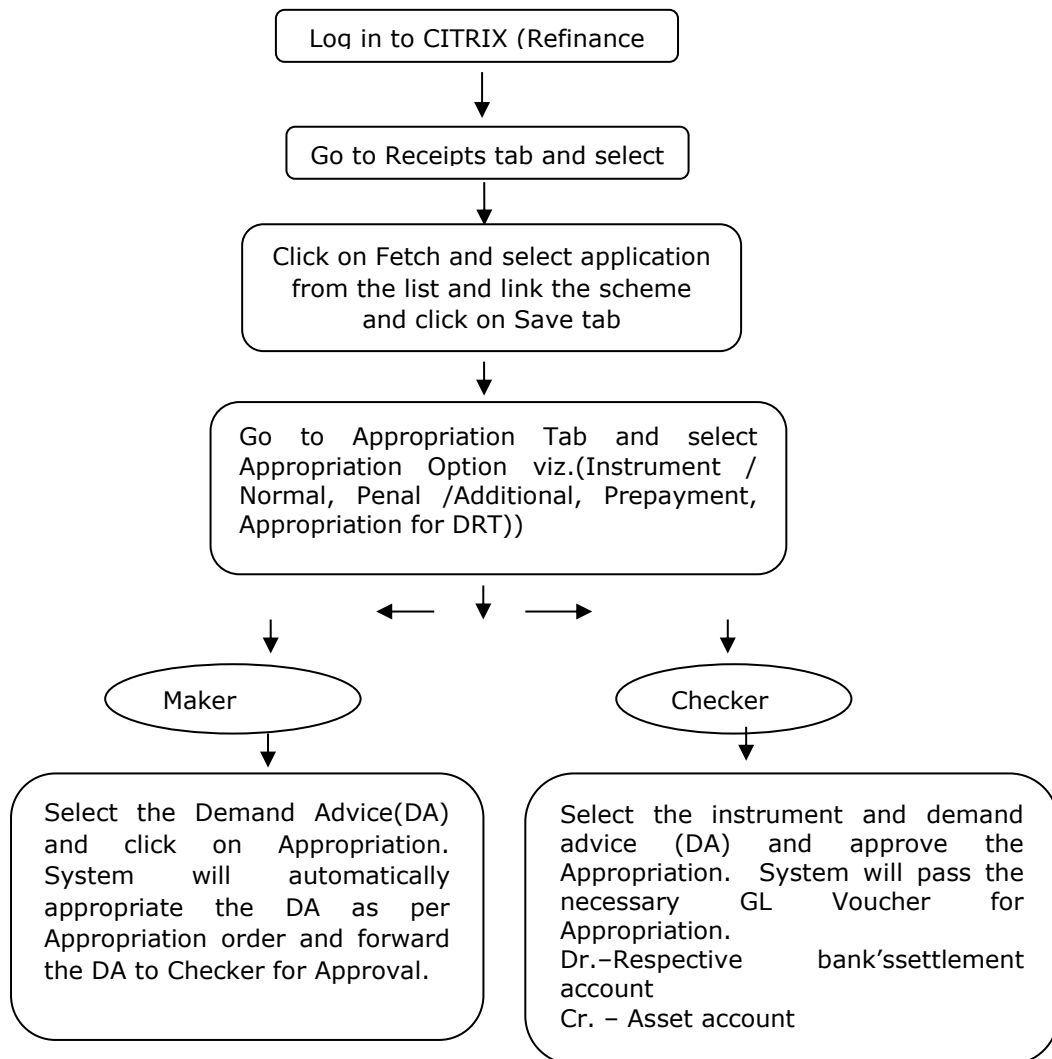


**iv. Refinance to BANKS – Follow – Up & Monitoring**



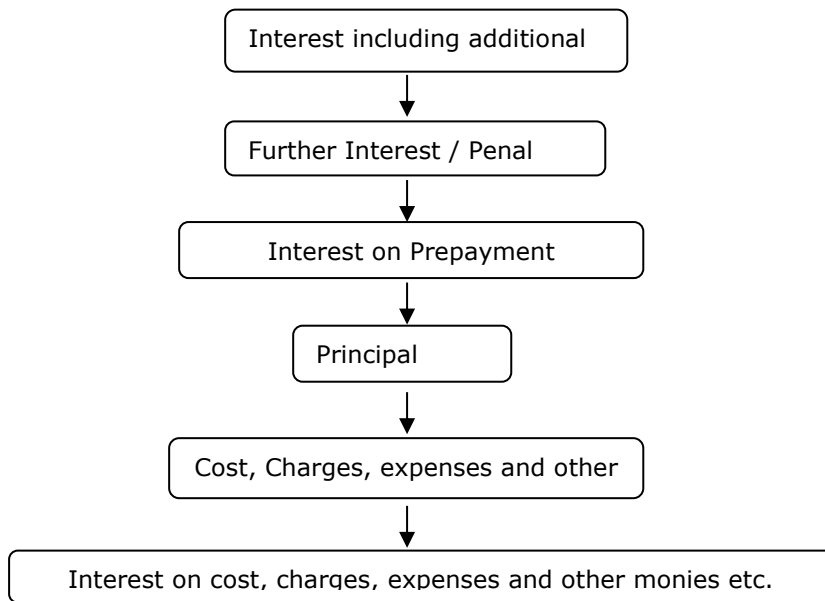


**\* - Under the specific schemes the repayment due dates of principal and interest are different.**

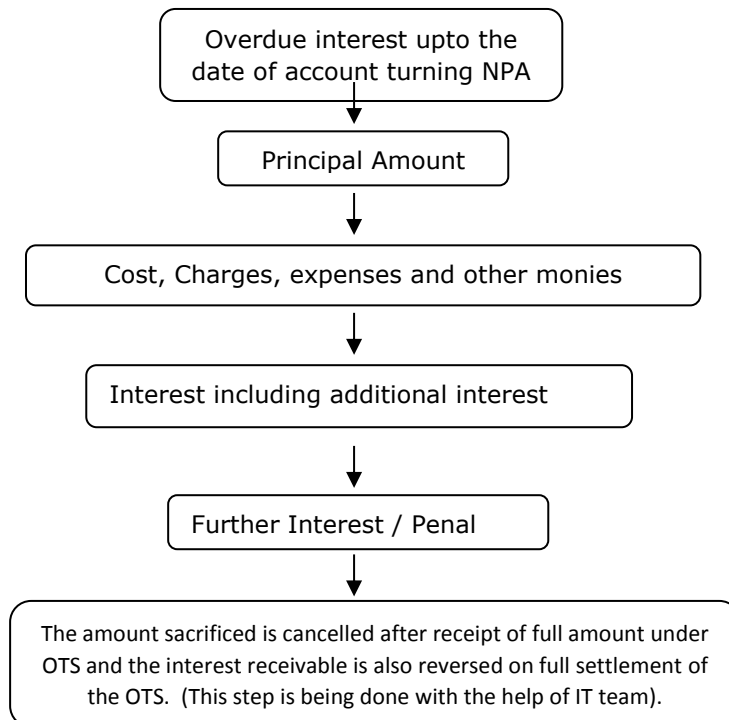


## **Order of Appropriation - (Refinance – Banks)**

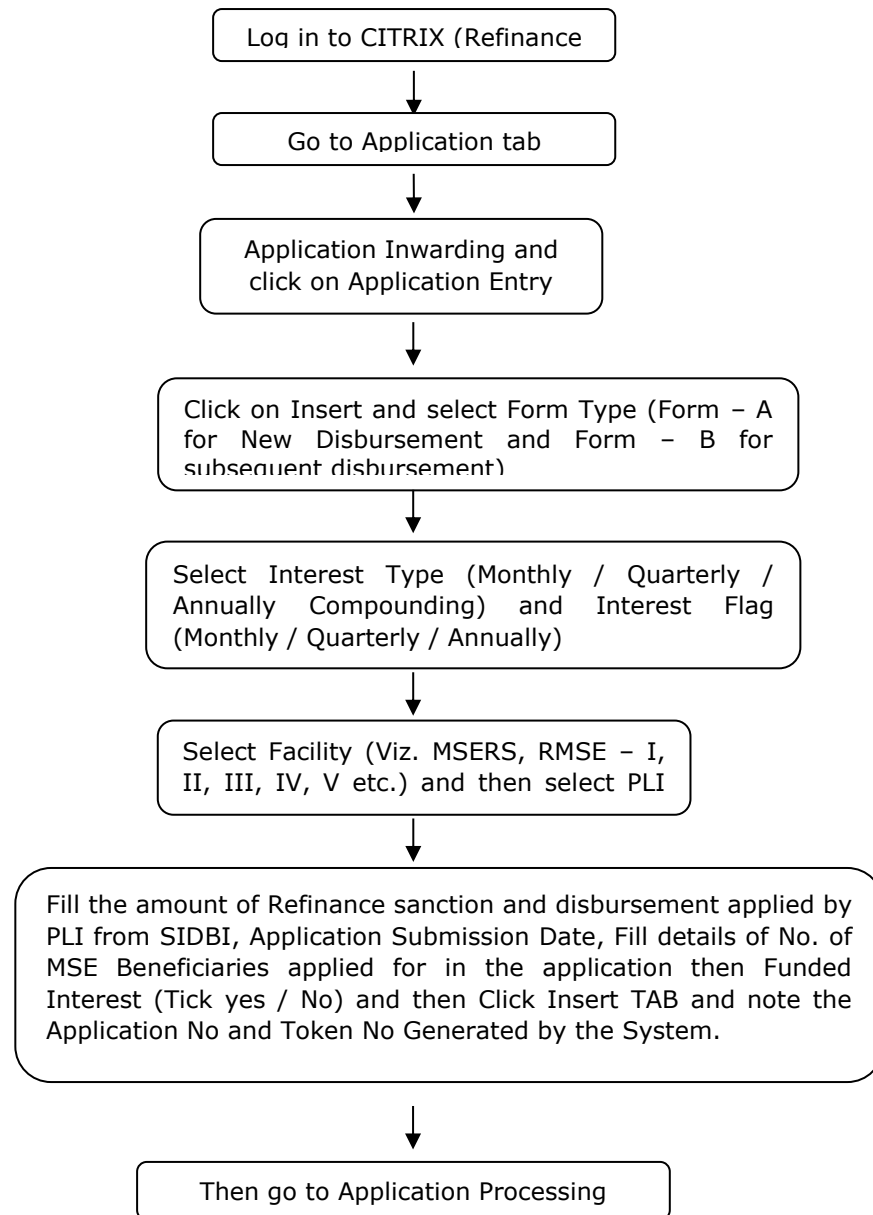
### **i. In the case of Standard Accounts**



### **ii. In the case of NPA Accounts**

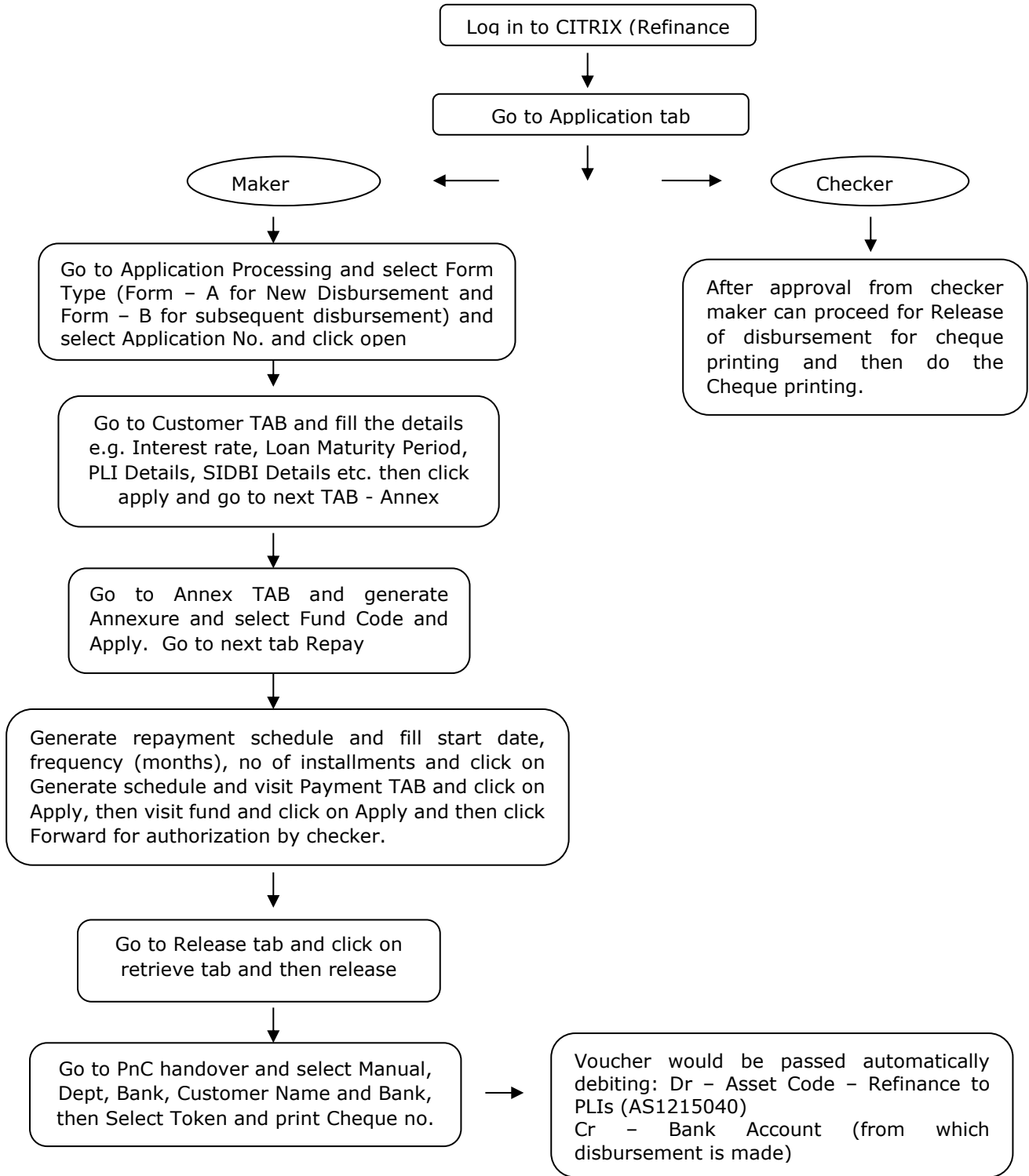


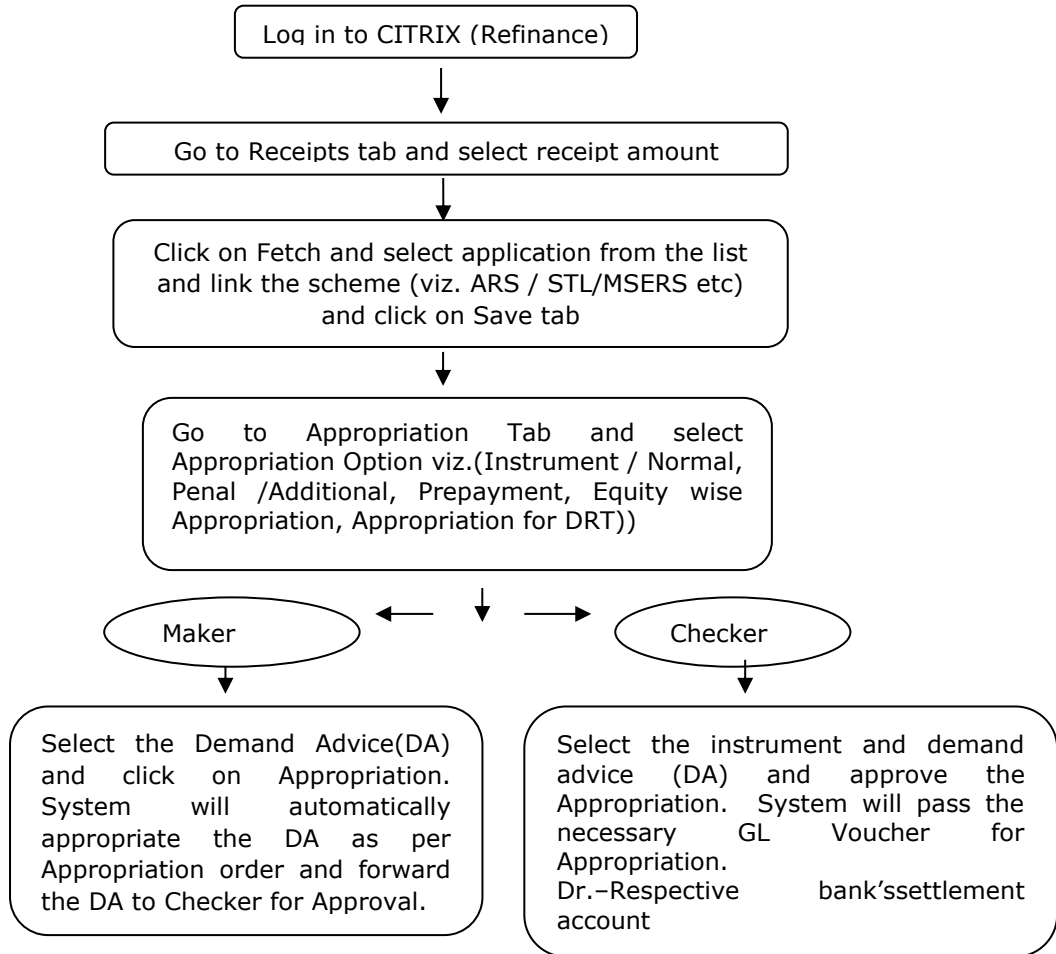
**System Flow Chart – Application Inwarding**



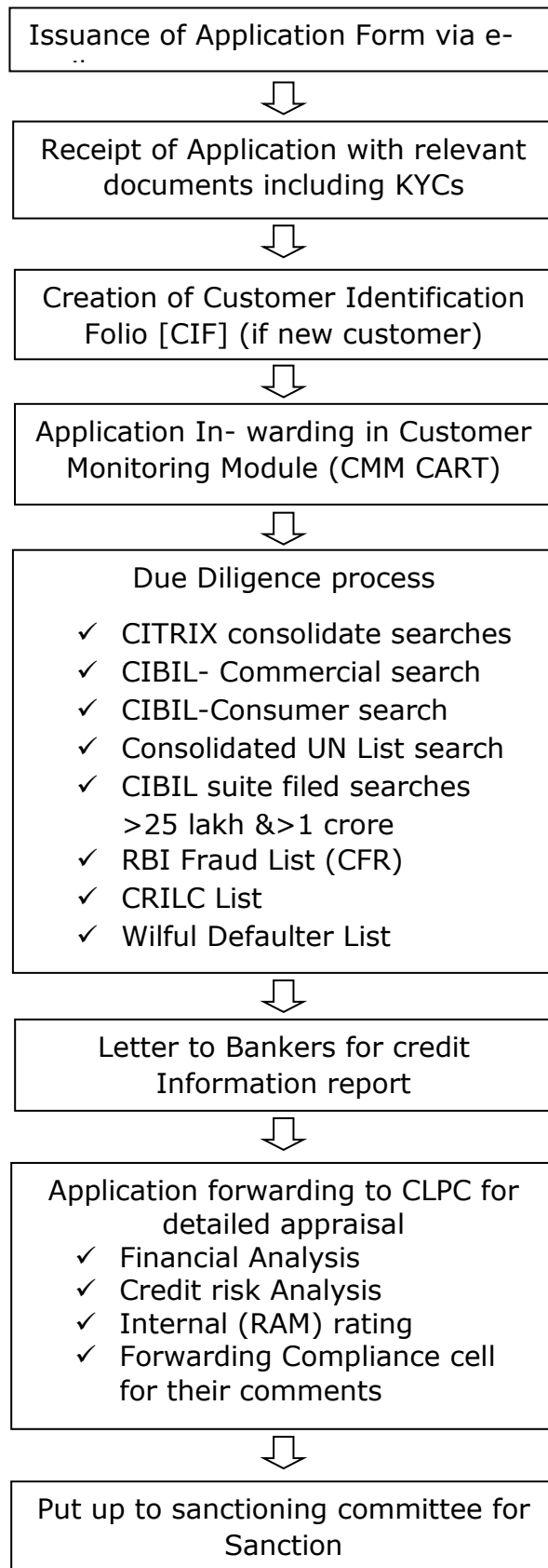
**Annexure - I**

**System Flow Chart – Application Processing / Disbursement**

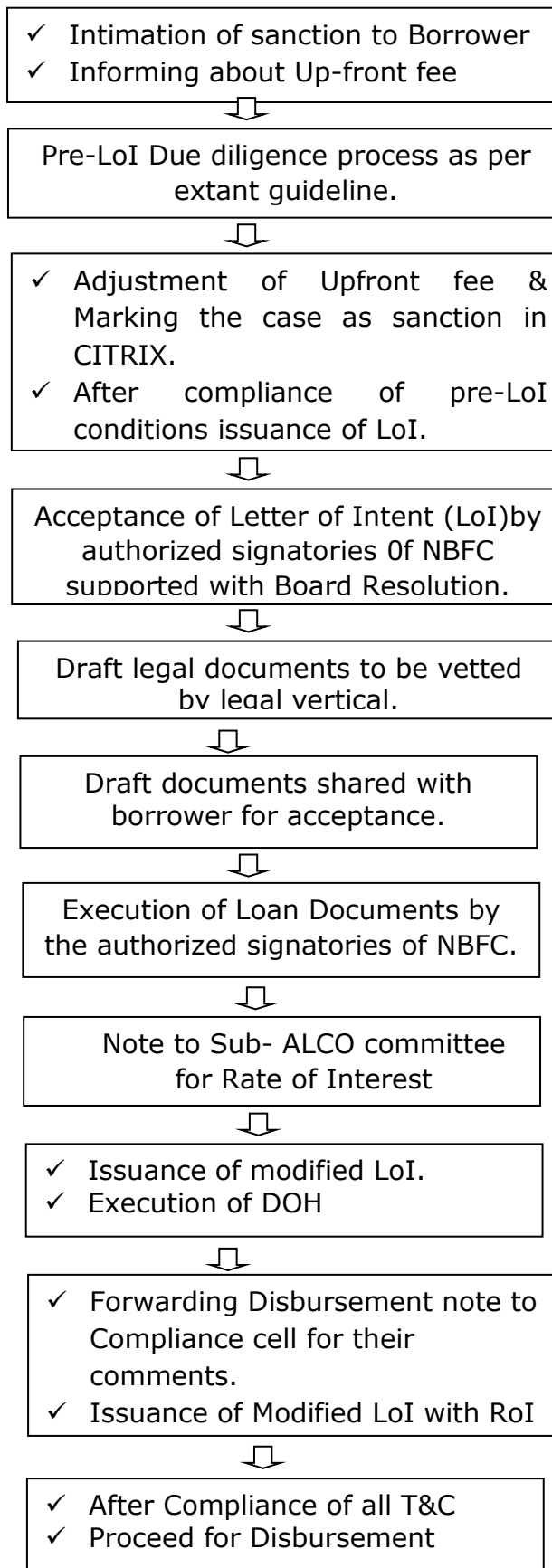




## IFV-NBFC-SANCTION



IFV-NBFC – Post San.



## **Refinance to Small Finance Banks Workflow**

### Pre – Sanction.

- i) Application for Refinance from the SFB.
- ii) Creation of CIF for new Customers.
- iii) Application Inwarding in CART - Application Monitoring Module.
- iv) Application forwarded to the CLPC for Appraisal.

### Sanction

- i) Due Diligence by the concerned RM / CLPC as per the extant guidelines.
- ii) Appraisal by CLPC.
- iii) Appraisal forwarded to RiMV for review rating and Risk concerns
- iv) Appraisal after addressing the risk concerns is forwarded to Compliance Cell for clearance.
- iv) Sanction / Rejection by the Sanctioning Authority.

### Post - Sanction

- i) Receipt of Sanction Minutes by the Dept.
- ii) Sanction / Rejection Intimation to the Borrower & Receipt of Upfront fees.
- iii) Issue of LoI post compliance of Pre-LoI conditions.
- iv) Acceptance of LoI – Terms & Conditions.

### Documentation

- i) Execution of General Refinance Agreement and letter of Authority (One time agreements)
- ii) a) RSFB - Acceptance of LoI & execution of Loan Agreement.  
b) RMSE - Acceptance of LoI.

### Disbursement

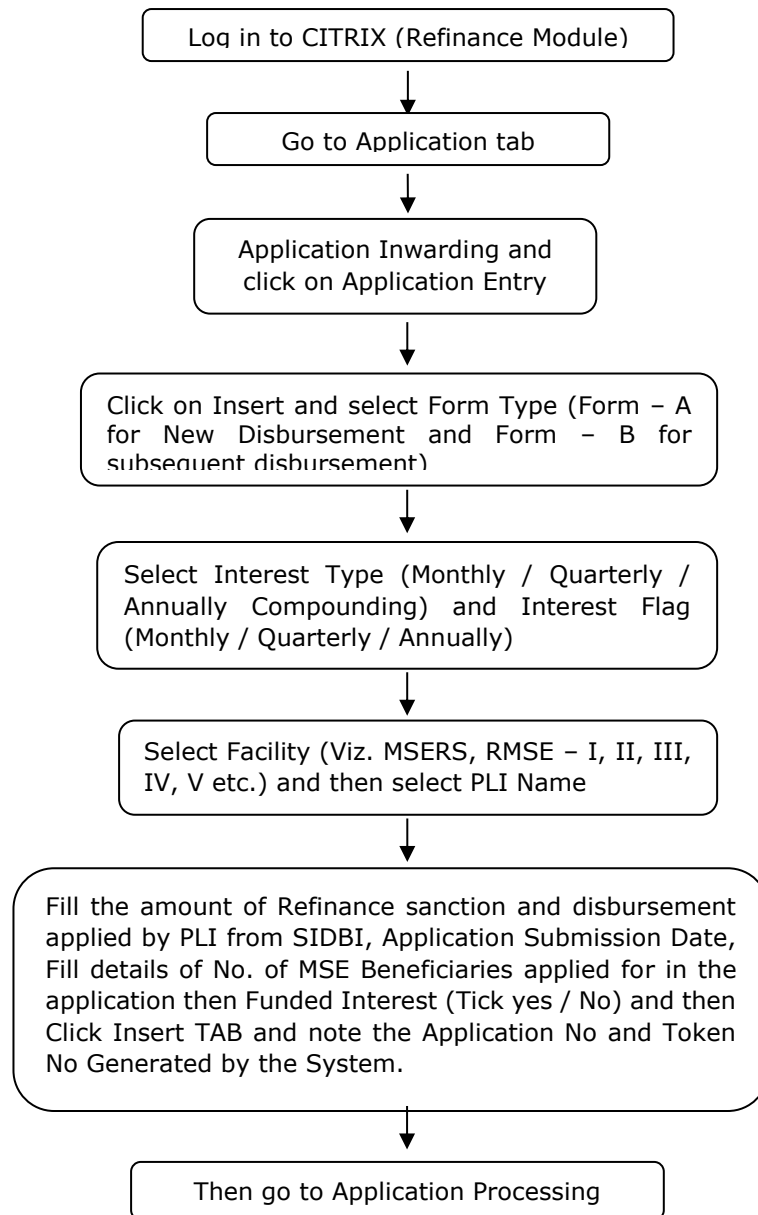
- i) Disbursement Request along with beneficiary list of the borrower against which refinance is availed.
- ii) Finalisation of Rate of Interest by ALCO .-[ For RSFB only]
- iii) Issue of modified LoI advising interest rate .-[ For RSFB only]
- iv) Examination of the list of beneficiary , check for compliance of T& C and approval of disbursement
- v) Disbursement Note forwarded to Compliance Cell and request for transfer of funds to treasury (Funds)
- vi) Disbursement to the Borrower.
- vii) Acceptance of Repayment Schedule.

### Follow – up Monitoring

- i) End – Use verification (Post - Disbursement Visit to the Borrower's Beneficiary units).
- ii) Quarterly Monitoring Report.
- iii) Half – yearly Book Debt Statement.
- iv) Annual review of the SFB's.
- v) RoC/ Closure of Accounts / Request for BCC's.



**System Flow Chart – Application Inwarding**



**Annexure - B**

**System Flow Chart – Application Processing / Disbursement**

