Annex

Baseline Requirements for the NPA classification Solution

I. Data Input

1. Data Input in the system by any means should be fully captured and stored without truncation [For example, time stamp - with date and time, narration field, or any other text data captured].
2. Ensure presence of necessary validation/verification checks in the solution for the user inputs, wherever applicable. Such validations, among other things should check for data type validations, min/max value, exceptions, etc.
3. Ensure necessary data validation/checks in the system for the data keyed in manually, wherever applicable. For example, such validations with master data (or parameters used in asset classification fed into the system as per the internal policy of the bank) could prevent issues related to incorrect entries generally seen (illustrative but not exhaustive list) in margin setting, moratorium period, security valuation, repayment schedule, products mapped/linked to different categories of account holders (as per applicability) etc.
4. Data input shall be effected only after authentication and authorisation.

II. User Access Management

5. Ensure that all "user-ids" in the solution have unique identification. If there are any generic user-ids used, it should only be used under exceptional circumstances and such ids should be mandatorily mapped to the employee ID of the user to fix accountability of the activities carried-out under the generic ID.
6. Provide for two-factor or higher level of authentication for the users of the application.
7. Restrict the access to the solution on "need to have/least privilege" basis for all users.
8. Provide for maker checker authorisation /control for transactions (an illustrative list of transactions includes updating/modifying the internal accounts, customer accounts, parameters – both financial and non-financial that affect the status of the credit portfolio/loan/asset.) entered in the solution. This shall also include transactions/activities carried out by administrator accounts in the application. (For example: Activities such as create/update/modify user-ids, roles, privileges including access rights to various modules; system related activities including updates to master data, etc. should have at least two individuals to complete the activity).

III. Straight Through Processing (STP)

9. Provide for straight-through processing (STP) and support for STP integration with all critical systems/add-on sub-systems/modules etc., in a seamless and secure manner for NPA/NPI classification as per extant guidelines on IRAC. Such STP mechanism shall seamlessly take into account all the facilities availed by a given customer (in case of advances) and all the instruments of an entity (where bank has made investments in an entity), maintained across multiple systems of the bank without any manual intervention. Further, banks shall also ensure that the updated account status, including asset classification of the customer accounts, flow to the CBS automatically, if NPA classification process is performed outside CBS.

IV. Back-end Data Access Restriction

10. Any changes to the data, parameters from backend shall be avoided. The solution should provide for changes to the data items only through front end (from the application (Ex: CBS) itself and not through the backend database update) after requisite authorisation. Audit trails/logs of access, changes to any data, parameters, if any, should be captured with specific user details in the system.
11. In case of exceptions in rare circumstances, such changes should be duly approved at an appropriate level and documented. Provision for MIS report should be available to auditors to generate complete list of back-end access and changes made.

V. Audit Logs

12. Provisions of audit trails/logs to capture details of mandatory fields (that are essential to complete the transaction and essential to identify the transaction for audit/forensic purpose in the future) of all the transactions (financial and non-financial) shall be made.
13. Logs should be maintained for changing the master data. System generated activity logs of the users with administrative privileges should also be maintained.
14. Secure storage and retention of logs in encrypted format with access controls in an archival solution.

VI. System Generated NPAs

15. All parameters required for NPA/NPI identification shall be captured in the CBS or associated sub-system(s)/module(s) meant for NPA/NPI identification/classification of asset codes as per Income Recognition and Asset Classification (IRAC) norms and extant instructions. It should provide for separate MIS report capturing all parameters for NPA/NPI identification. Such parameters could either be configured in database or application itself as per the architecture of the solution/sub-system.

VII. Test Environment

16. The existing test environment in the bank with dummy data and functional logic similar to that of the product environment of the solution shall be made available to the supervisors during their onsite supervisory visit(s) as per the requirements. This shall be required, *inter alia*, to perform sample transactions review to assess whether the solution adheres in complying with regulatory prescriptions in the extant environment for NPA/NPI identification as per applicability.

****