**Business Requirement Specification for Change Request**

|  |
| --- |
| 1 GENERAL INFORMATION |

* 1. Name of the project : Fraud Risk Register
  2. Initiating group name & code : FCPG
  3. Cost centre : FPC
  4. Name of Application Impacted : FMS
  5. Name of module(s) in the above

Application that would be impacted : FMS-RCU

* 1. Contact person from initiating group

In case of doubts/clarifications:

Name : Vaibhav Desai

Employee no. : 351620

Designation : MI

Reporting authority of contact person:

Name : Sunil Mandhyan

Employee no. : 140300

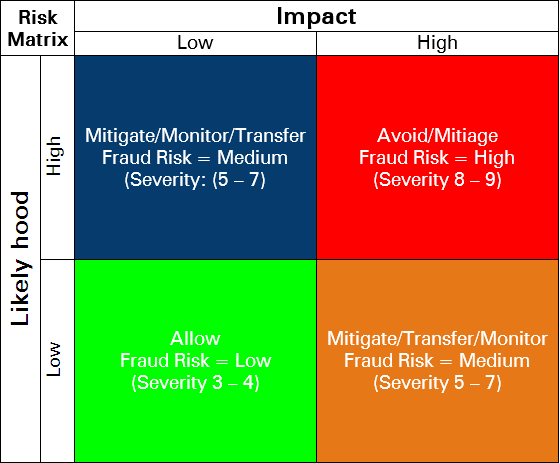
Designation : CMII

|  |
| --- |
| **2 DETAILED INFORMATION** |

* 1. **Business Requirement:** ICIC bank is a leading private sector bank with myriad products and processes ranging from Retail & Corporate Assets and Liabilities businesses. The Financial Crime and Prevention Group (FCPG) is bestowed with the responsibility to review, assess and recommend measures to mitigate fraud risk across all the products and processes within the bank.

Risk Grading is carried out by FRAP managers post process reviews and walkthroughs. The primary objective is to highlight the mitigates already in place, residual risk and capture likelihood and impact of fraud risk and recommend new mitigate to stop/curtail frauds. Likelihood and Impact is captured as Low, Medium or high.

Following diagram shows how fraud risk is arrived at:



Constraints with present working:

1. The Risk grid is prepared and maintained manually.
2. Final Fraud risk is given manually and is based on judgement of the assessor.
3. Currently all the risk assessments are stored in respective assessor’s PC and at time it becomes difficult to retrieve if the assessor is not present.
4. The reverts on recommendations and timelines is maintained manually
5. Follow-ups are done on best effort basis.
6. Risk Assessments for Amendments in product and process is done all over again as previous Risk Assessment may not be available.

With increasing products and processes, risk assessments, changing times and stakeholders there have been challenges with regards to “Record Retention” of risk assessments made by respective FCPG FRAP group members. Presently, it is managed by respective product and process manager on their desktop.

**Proposed System:** The purpose of this proposal is to have a prepare risk grid, provide likelihood and Impact rationale, Auto calculating the risk grid using Risk decision matrix, Documenting recommendations, capturing revert from business teams against each recommendations along with timelines, following up with business team based on timelines provided. The system will also serve as template for Risk assessment, System will allow using earlier templates which can be used to carry out risk assessment of similar products/processes or changes in existing product and processes. System will have user friendly, simple and easy to use UI to record new risk assessment, update progress of recommendations.

Thus, System will be a centralized repository for all fraud risk assessments including risk grid, proposal documents, recommendations, memos/PAC and tracking the status of recommendations. The goal is to have 100% record retention of all the products and processes reviewed by the FCPG FRAP.

**Scope:** All products and processes reviewed by FCPG FRAP teams including digital channels, cards, branch, operations, phone banking etc.

**2.2 Interface & Functional Requirement**

1. LAM based front end access for users with Windows NT based login
2. Role based customized functionalities as administrator, read only, read and write etc. Restricted and Selective access to Risk Grading Matrix based on Product/process i.e. Digital Channel, Cards, Liabilities, Phone Banking, Operations, Etc. **Refer Annexure I LAM ACM** for Access Control Matrix
3. System should have following menu options:
   1. RiskGrid
      1. New - Blank Template
      2. New – Select Existing RiskGrid as new template
      3. Modify – Existing Open proposal
      4. Modify – Existing Closed Proposal (System Admin Only)
      5. Delete – Closed Proposal (System Admin Only)
   2. Recommendations Updates
   3. Search and Query
      1. Search RiskGrid using
         1. SR No.
         2. iMemo Number
         3. Product/Channel
            1. Proposal Name
            2. Risk Rating
            3. Deleted Records
      2. Recommendations Pending
         1. Product Channel Wise
         2. Follow-up Date wise
         3. Recommendation Status wise
         4. Implementation Date wise
   4. Logout: On Click to logout the user should be logged out of the system.
4. To prepare a RiskGrid user can select
   1. **New – Blank Template:** A Blank Template should be open where data entry for all the field will be done by the user. User should be allowed to make changes to all the fields.
   2. **New – Select Existing RiskGrid as new template:** User will be asked for Risk Grid Reference number or select the proposal by selecting Product / Channel and then by proposal Name <Quick search/Filter by entering the proposal name should be provided along with Dropdown. This will include the open and closed proposal>. User should be allowed to make changes to all the fields. Note: No changes will be saved for closed proposal.
   3. **Modify – Existing Open Proposal:** User will be asked for Risk Grid Reference number or select the proposal by selecting Product / Channel and then by proposal Name <Quick search/Filter by entering the proposal name should be provided along with Dropdown>. User should be allowed to make changes to all the fields.
   4. **Modify – Existing Closed Proposal (System Admin Only):** User will be asked for Risk Grid Reference number or select the proposal by selecting Product / Channel and then by proposal Name <Quick search/Filter by entering the proposal name should be provided along with Dropdown>. User should be allowed to make changes to all the fields.
   5. **Delete – Proposal (System Admin Only):** Both open and closed proposal will be in scope for deletion. User will be asked for Risk Grid Reference number or select the proposal by selecting Product / Channel and then by proposal Name <Quick search/Filter by entering the proposal name should be provided along with Dropdown>. User should be prompted that proposal will be deleted permanently. If the user Selects “Yes”, The proposal should be marked as deleted. However, the same should be available in database. However, the reference number and proposal name should not be part of any search options other than search for deleted records and capture record deletion date.

The Risk for the New / modification in product/Channel needs to be captured in format in **Annexure II – RiskGrid.**

The User will select value from the dropdown list for the following fields from the dropdown. User will be asked to select the values from the list applicable for Product / channel by selecting the Check box. After selecting the values user will have to select Add to add the list to in respective field.

If any of the value is not available in master, then user will be required to update the values in respective master. User will be asked if the value will be applicable for which all product/Channel

Fields where above will be applicable are

1. Mitigation
2. Residual Risk
3. Likelihood Rationale
4. Impact Rationale
5. Recommendation

Benefits will be entered in Benefits field directly.

Transaction Type will be selected using Drop Down (Only One value from the drop down)

Likelihood will be selected using Drop Down (Only One value from the drop down)

Impact will be selected using Drop Down (Only One value from the drop down)

Fraud Risk will be calculated basis the Transaction Type, Likelihood and Impact selected

Fraud Risk Conditions:

|  |  |  |  |
| --- | --- | --- | --- |
| Transaction Type | Likelihood | Impact | Fraud Risk |
| Any | Low | Low | Low |
| Any | Medium | Medium | Medium |
| Any | High | High | High |
| Financial or Critical | Low | Medium | Medium |
| Financial or Critical | Medium | Low | Medium |
| Financial or Critical | Low | High | High |
| Financial or Critical | High | Low | High |
| Financial or Critical | Medium | High | High |
| Financial or Critical | High | Medium | High |
| Non Financial or Non Critical | Low | Medium | Low |
| Non Financial or Non Critical | Medium | Low | Low |
| Non Financial or Non Critical | Low | High | Medium |
| Non Financial or Non Critical | High | Low | Medium |
| Non Financial or Non Critical | Medium | High | High |
| Non Financial or Non Critical | High | Medium | High |

Severity will be calculated based on the values selected in Likelihood, Impact and calculated fraud risk

Low will be assigned value 1

Medium will be assigned value 2

High will be assigned value 3

For Example:

1. If the likelihood is Low, and Impact is Low and Fraud Risk is also Low then Severity will be 3 (1+1+1)
2. If the likelihood is high, Impact is Medium and Fraud risk is also High then Severity will be 8 (3+2+3)
3. If the likelihood is Low, Impact is High and Fraud risk is Medium then severity will be 8 (1+3+2)

On saving the proposal, System should check if the proposal Status is ‘Closed’.

* + 1. If Proposal Status is ‘Closed’, User should be prompted that changes will not be Allowed. Do you wish to continue (Y/N).
       1. On Selecting Yes, New reference should be generated and proposal should be saved.
       2. If user Selects No. Then should be prompted to change the proposal Status. No further action required, Existing proposal will be displayed.
    2. If proposal Status is ‘Open’. New reference should be generated and proposal should be saved.

For Saved and Closed Risk Grid, the user will be provided option to export the RiskGrid in Excel or PDF format. Refer Annexure IV for Export RiskGrid format.

1. **Recommendations Update:** 
   1. The Users should be allowed to search for Recommendations and update the same. User Will be prompted to enter the following
      1. Check box to select Recommendation Status “Pending”, “Implemented”, “Dropped”.
      2. To filter the records, user can enter dates. For pending and Dropped the date will be Recommendation date and for Status Implemented the date will be implemented date.
      3. To filter further, User can also select the Product/Channel and Proposal Name.
      4. Search using Risk Grid Reference Number.

Except the checks box all other fields will be optional.

The output will display the list of recommendations pertaining to the products and channels the user has access to.

The user will be able to select the recommendation through click on the recommendation reference number and update the same.

User will be allowed to make changes to all fields under recommendations and save the record.

Once the recommendation is implemented it should be updated in all linked RiskGrids.

1. Apart from fields mentioned in the Annexure II following should also be captured to maintain logs. These fields should also be applicable for all masters mentioned in Annexure III.

|  |  |
| --- | --- |
| **Field** | **Rationale** |
| Record Creation Date and Time | Date and Time of Record creation |
| Record Created by | Employee ID of User creating the record |
| Record Modified Date | Date and Time of Record Modification (To be captured if there is any changes made and saved in the existing riskgrid). |
| Record Modified by | Employee ID of User Modifying the record. (To be captured if there is any changes made and saved in the existing riskgrid). |
| Record Access Date and Time | Date and Time of Record Access (To be captured if riskgrid is accessed through read only mode or through modified role but closed without saving). It should also be captured if the record is access and session is terminated without saving the RiskGrid. |
| Record Access by | Employee ID of the User Accessing the Riskgrid. It should also be captured if the record is access and session is terminated without saving the RiskGrid. |

The Logs should be stored on incremental basis and not just for last modified or last access. For every modification, User should be prompted to enter the summary of modifications made in the risk grid > Field Modification details. The details should be stored separately for each risk grid and should be available in reports.

1. Search and Query options: User should be shown options to search RiskGrid or recommendations.
   1. Search RiskGrid using
      1. SR No.: User is asked to enter the SR No. only.
      2. iMemo Number: User is asked to enter the i-memo number
      3. Product/Channel: User is asked to enter the following:
         1. Product/Channel > Proposal Name
      4. Risk Grid List: Enter Date range and Select the RiskGrid Status: Open or Closed or Deleted (Check box). Date will be RiskGrid creation date and time.
      5. Risk Rating: List all Proposals having Likelihood = <High/Medium/Low>; Impact = <High/Medium/Low>; Fraud Risk = <High/Medium/Low>; Severity = <3 to 9>; None of the fields is mandatory. However, at least one field selection is mandatory. Fields not selected are to be ignored. For selected fields, Query will work using AND operator.
      6. Deleted Records: User is asked to enter the following:
         1. Product/Channel > Proposal Name or
         2. User Should be asked to select date range to list all proposals deleted within the date range. (Deleted Date)
   2. Search Recommendations
      1. Search Recommendation Status <Pending/Implemented/Dropped/> Multiple selection through Checkbox (Mandatory)
      2. User will be prompted to enter the Date Range (Mandatory)
         1. For pending and Dropped the date will be Recommendation date and for Status Implemented the date will be implemented date.
      3. Select Product Channel Wise <Drop Down> (Optional) Multiple choice.

Export / View functionality should be provided for all Search and Query option. For Export Option, user should be asked export to Spread Sheet or PDF.

* 1. Automated publishing of dashboards / risk grids / MIS to predefined stakeholders
  2. Fields / Tabs will be required to update details related to respective product and process risk grading
  3. Provision to send E-mail notifications
     1. New risk register is created
     2. Monthly / Quarterly review to the creator and owner
     3. Provision should be made to manually tag frequency of review for any given product or process
     4. The authority to change the frequency should be with the vertical head / administrator
  4. Search functionality to make it user friendly and easy to locate risk assessments

1. Other functionalities.
   1. Provision to attach documents related to product and processes PAC/Proposal note / MEMO / Minutes) etc.
   2. Audit trails of user activity and changes made to risk grading. Audit trail should be appended and not overwritten.

Sample fields that should be displayed based on above selection,

**Sample – Risk Grading Matrix**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Corporate Banking: Payment Instructions through EMAIL** | | | | | | | | | | |
| **Channel** | **Mitigates** | **Residual Risk** | **Likelihood** | **Impact** | **Fraud Risk** | **Severity** | **Recommendations** | **Revert on recommendations** | **Likelihood Rationale** | **Impact Rationale** |
| Email | **Email Instruction** 1. Registered email ID / FAX of corporate (NBFC) 2. Standardized format / Letter Head for each NBFC (Refer formats given by the NBFC) 3. Calling the authorized signatory for confirmation on transaction | 1. Business Email Compromise 2. Email Spoofing 3. Forgery 4. Phishing  5. Crimeware | **High** | **High** | **High** | **9** | 1. Emails should be digitally signed  2. Standardized format in which the instructions should be taken 3. Dedicated group ID for NBFC and bank through which communication will happen **4. Validate letter head on which the requests has been received** 5. Instructions should be received from company domain from authorized email accounts and not open source email services such as Gmail, yahoo etc. 6. Verify sender domain while replying the email instruction to ensure the email is not spoofed 7. Reporting mechanism / process where suspicious request is established 8. Seek approval from ISG for the process 9. SMS & Email alert on receiving instructions | 1. This is not feasible 2. Each of the NBFC is currently using a standard format at their end (we will verify instructions received vis-à-vis their standard format), however their format may undergo slight variations with transactions which we would have to accommodate 3. We will create a separate group ID 4. Incorporated in revised process note 5. Incorporated in revised process note 6. Incorporated in revised process note 7. Incorporated in revised process note 8. Initiated for approval, will share once received | **A. Business Email Compromise / Email Spoofing / Forgery / Phishing / Crimeware /  1. Business Email Compromise (BEC)**  - E-mail accounts can be compromised through Phishing & Crimeware **2. Email spoofing**  - Fraudsters can spoof email ids so that the message appears to have originated from authorized email id **3. Forgery**  - Forged letter head and signature  - Scanned documents can be forged and sent through E-mail (Signature ovelay on the scanned document) **4.** **Phishing & Crimeware:** Customers personal and banking credentials like User ID, Password etc. can get compromised through targeted attacks of,  a. Phishing, b. Malware/Trojan c.Increasing trend of Android related vulnerabilities d. Rogue apps stealing critical information such as user id, password, banking and email credentials - NRI fraud trend experienced in FY17, customers have been vulnerable and fallen prey to phishing and e-mail hacking related frauds - With advent of smartphones, fraudsters can simulate campaigns similar to once by ICICI bank and target customers with links sent through emails - The links have the potential to install malware and also seek banking credentials from customers in the name of bill payment/online security etc. - Targeted customers would end up compromising their email and banking credentials in the name of security, aadhaar update, bill payment etc. | 1. Reputation Risk due to negative posts on social / print media etc. 2. Crimeware has capabilities to steal information (Personal and Financial) 3. Financial loss to to extent of account balance and transaction limits 4. Liability clause with NBFC to ensure bank is not held liable in event of email compromise and negligence at clients end **(Email/fax indemnity will be obtained from all NBFCs and same will be part of escrow agreement for every funded project – legal document to cover from any potential loss)** |

**Frequency**: Real-time

**Path where flat file will be placed**: Ask User to export in Excel or PDF format. User to be asked for path where Risk Grid is to be saved.

**Incremental condition**: Nil.

**File name convention** : Concatenate SR No., Proposal Name

* 1. **Benefits envisaged from the proposed changes in terms of cost / man- days saved / risk mitigation etc. :**

**Benefits: Financial:**

Approximately ₹72,000 per annum on Productivity Savings

Refer Cost Benefit Sheet in Annexures to BRS.

**Benefits Non-Financial:**

* Central Repository.
* Continuity: Not dependant on individual manager.
* Ease in retrieval.
* Confidentiality
* Reports
* New Versions update to have trail of how risk have changed over a period of time.
* Standardize and effectively handle process / activity
* Improve productivity by accelerating review process and data retrieval
* Enable achievement of service levels
* Continuity: Not dependant on individual manager.
* Reports will provide overall picture events happening in the system
* Provide MIS reports / dashboards to seniors

* 1. **Risk Analysis from Process / product Perspective:** Nil
  2. **List out any specific Interface Requirements:** Nil
  3. **Please specify test scenarios for testing of the functionality –** Will be provided after approach is finalised.

**SL No Test Cases Test Details Expected Results**

*UAT and data validity for correct details present in BIU database in relation to total count of cards and their status.*

The Test case scenario document shall be shared separately

## 2.7 Functionalities / Modules (Ignore if no impact on functionalities. Else please describe the following for each new functionality, or for changes in any existing functionalities)

|  |  |  |
| --- | --- | --- |
| 1 | Description | Description of the function / module covered |
| 2 | Assumptions | Specific assumptions with regard to this module |
| 3 | Functional Requirements | Inputs - that are either given by the user invoking this function or those retrieved from within the system  Process - the procedure and major validations performed  Outputs - these include the various transactions, reports and queries that will be generated |
| 4 | Interfaces   * Internal * External | Any information if required from other modules for the functioning of this sub function will be regarded as an interface-input.  Any information from this module that will be used by other modules will be regarded as interface-output. |
| 5 | Communications | Data transfers required, if any. |

**2.8 Priority**: HIGH

**2.9 Security Requirements and Testing**

*(Security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling should be defined here.*

As per the ISG norms

|  |
| --- |
| **3 REPORTS** |

## (Ignore if no impact on reports. Else please describe the following for each new report, or for changes in any existing reports).

**Refer Annexure V – Reports**

* 1. Report Name:
  2. Frequency (Daily / Monthly)
  3. Selection Criteria
  4. Sort Order
  5. Processing (Brief on processing to be done in the report)
  6. Information (Mention fields to be printed with grouped properly)
  7. Consolidation (Mention summary information, group totals, grand totals, if any)
  8. Format of the report with dummy data (as close to actual data as possible)

|  |
| --- |
| **5 Date by which the project needs to go live: ASAP** |

|  |
| --- |
| **6 Name and designation of Business user head: Pinaq Dudhawala** |