White Paper

Operations Risk Management

RCSA Management and Analysis

iCreate | BANKING INTELLISENSE

WE PUT THE BANKING INTO BUSINESS INTELLIGENCE

www.icreate.in

Operations Risk Management

RCSA Management and Analysis

1. Introduction

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events. It includes reputation and franchise risk associated with a bank's business practices or market conduct. It also includes the risk of failing to comply with applicable laws, regulations, Regulatory Administrative Actions or bank's policies. Operational risk does not include strategic risk or the risk of loss resulting solely from judgments made with respect to taking credit, market, interest rate, liquidity, or insurance risk.

The objective of the RCSA (Risk Control Self-Assessment) and Operational Risk Policy is to establish a consistent framework for assessing Operational Risk and the overall effectiveness of the internal control environment across the bank. While RCSA data can be used to compute capital charge for operational risk, it is the building blocks for Advance Measurement Approach (AMA) under Basel II guidelines.

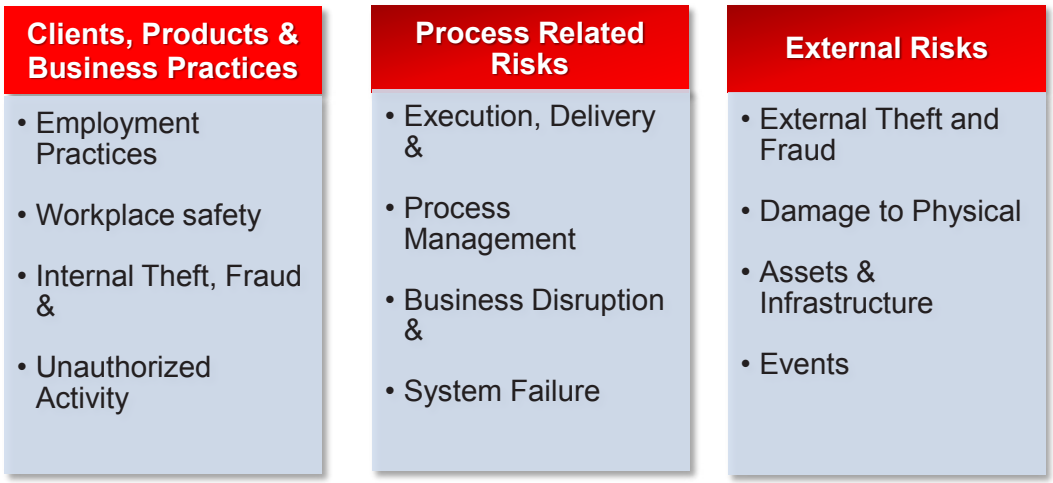
2. Objective

This document has two objectives:

- Firstly, to explain the concepts of RCSA and lay the basic guidelines for developing templates for RCSA entities. This component is business oriented and defines the organization structure, risks and controls at each RCSA entity and assigns ratings for the same.
- Secondly, to outline the process of RCSA tracking which will capture RCSA information and help compute capital charge for Operational Risk. This data will form the basis for computation of operation risk capital charge using AMA approach.

3. Operational Risk

Operational Risk can be divided into three categories as shown below:



There are a number of incidents (called Loss Events) which occur in all the above categories. They can occur in any unit in the bank like a branch, IT department, Sales department, Controls department – it can occur in any department irrespective of whether it is a profit centre or loss centre. Each incident will have an associated monetary loss value associated with it. The frequency of loss events could be mitigated by controls and constant measurement can result in computation of an average loss frequency and average loss value for a given period of time. Projections based on these numbers using statistical tools could help us in computing the capital charge as described in later sections of this document.

4. RCSA Process

RCSA is a dynamic and iterative method for identifying important operational risks and Key Controls and for assessing and reporting on their effectiveness for each RCSA entity. When breakdowns in the controls environment are identified they are proactively tracked until fixed.

The key points to note are:

- It is dynamic. It keeps changing all the time based on controls introduced by the unit
- It is iterative – one puts controls, sees its effectiveness and changes it, if is not effective
- It is done at an RCSA entity (unit) level and all RCSA for entities (units) in an entity are put together to come up with an RCSA for the entity. Thus all departments in bank can be RCSA units and one can consolidate the RCSA and come up with an RCSA rating for the bank
- Corrective actions are tracked and implemented continuously

Typically, an organization implementing the RCSA processes will go through the steps described below.

Documenting & Defining	Identifying	Assessing & Assigning	Reviewing & Approving
1. Document the overall internal control environment	4. Identify RCSA Entity-Level Important Risks	6. Assess (Test) and Rate Key Controls against Important Risks	Review RCSA templates after testing is completed and approve RCSA results
2. Identification of 'Top-Down' Important Risks	5. Identify Key Controls	7. Create Corrective Action Plans (CAPs)	
3. Define RCSA Entity		8. Assign a Risk & Control Rating to each Important Risk on a residual basis	
		9. Assign a Risk & Control Rating to the RCSA Entity and report RCSA information as required	

4.1 Documenting and Defining

The first step is to define the organization hierarchy and make a list of top level risks for the organization. Based on the organization hierarchy, we can define the RCSA entities or units which will perform tests and measure risks, implement controls, measure their effectiveness and keep improving continuously. RCSA reports from all RCSA entities are submitted to the central group in the entity to arrive at an overall risk for the entity. The reporting entity defines top level risks and controls which percolate to lower units within the entity. Units can also add additional risks and controls if they are not covered by the entity level risks and controls. Let us see an example from the automobile industry and the same can be extrapolated for banking. It is a simplified case to understand the concepts.

Everyday Example — Documenting & Defining → Identifying → Assessing & Assigning → Reviewing & Approving

- We will look at the used car selling process of XYZ Motors, a car manufacturer. Its Entity-Level Controls are:

Entity-Level Controls (XYZ Motors)
- Mandatory use of original equipment replacement parts
- Manufacturer's training and certification of dealer's mechanics
- Manufacturer's pre-owned 200-point inspection program

'Top-Down' Risks (XYZ Dealership of New Jersey)
- Poor quality parts can result in short service life and customer dissatisfaction
- Improper maintenance/repairs can result in car breakdowns, unreliable performance and customer dissatisfaction
- Selling pre-owned cars that had been abused or in accidents will increase customer dissatisfaction
- A poorly trained sales staff can result in customers buying cars that do not suit their requirements

- RCSA Hierarchy:
  - **Entity:** XYZ Motors
  - **Sector:** XYZ Dealership of New Jersey
  - **Business:** Certified, pre-owned Auto Dealership
  - **RCSA Entity:** Pre-owned Auto Inspection and Repair

In the above example, when we want to evaluate RCSA of XYZ motors, we will have to take RCSA of all its divisions – we are now looking and Used Cars sales as entity which publishes Entity level controls and Risks and each RCSA entity will have to select and give data relating to number of incidents, loss value during a reporting period along with controls to minimize risks and their effectiveness. Within each RCSA entity you can have multiple Test Units. A RCSA entity will collate all results of test units under it for reporting – reporting is done at RCSA entity level.

4.2 Identifying Risk and Controls

Each unit will now evaluate the risks and controls under three important categories:

- Risks which come from top level entity
- Regulatory Risks
- Additional risks not covered by top level entity risks

Continuing with our earlier example, the three types of risk monitored by RCSA tracking unit will be as follows:

Everyday Example

- Continuing with our everyday example, let's see how Important Risks have been identified for the Pre-owned Auto Inspection and Repair.
- "Top-Down" Important Risk
  - A. Improper maintenance/repairs can result in car breakdowns, unreliable performance and customer dissatisfaction
- Regulatory Requirement
  - B. The risk of non-compliance with laws regarding sale of cars with hidden defects (Lemon Law, for ex.) can result in financial loss due to warranty claims and lost customers
- RCSA Entity Owner Identified Risk
  - C. The risk of selling damaged cars as "certified, pre-owned" can result in reputational damage

A RCSA sheet for Risk Management processes in a bank is provided as an example in the annexure.

4.3 Assessment of Risks and Controls

RCSA is used for tracking important or materialistic risks only. If there are risks which are identified by a unit as "not important or not materialistic", they must be documented and reviewed periodically. Managers of units reporting the RCSA are fully responsible for identifying risks, tracking incidents, associating loss value, linking them to risks, implementing controls to mitigate risks and report data in specified formats.

Controls are put in place in each RCSA entity to mitigate and eliminate risks. It is important to have periodic checks to see if the controls are effective are not. If the controls are found ineffective, a corrective action plan (CAP) must be put in place to mitigate risks. This must be a continuous process as risks change with changing processes and controls become ineffective from time to time and hence it is required to test periodically. Testing of controls can only be done on a sampling basis. The testing of controls must follow the following process:

- Select the appropriate sampling size
- Identify an independent tester to execute the test – someone other than the person performing the process or control on a BAU basis
- Summarize testing results for the completed tests
- Capture and document the location or attach evidence to prove the test's outcome
- Determine the control's operating effectiveness (e.g., Satisfactory, Not Satisfactory: Business Issue (BI), Not Satisfactory: Major Business Issue (MBI)

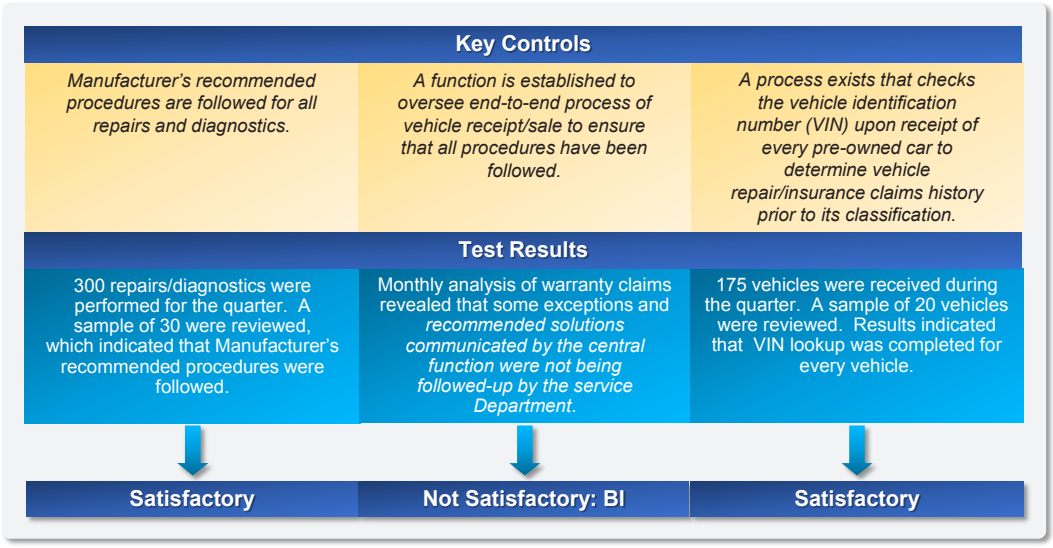
The following table summarizes the sample size required for effective testing of controls. It also gives the periodicity of testing required based on frequency of application of the control.

Control Frequency	Sample Size (per test)	Test Frequency
Recurring Manual Control	Lesser of 10% or 8	Quarterly
Recurring Manual Control	20 items or 100% if Pop is <20 (AsiaPac)	Quarterly
Daily	Lesser of 10% or 5	Quarterly
Daily	20 items or 100% if Pop is <20 (AsiaPac)	Quarterly
Weekly	2	Quarterly
Monthly	1	Quarterly
Quarterly	1	Semi-Annually
Semi-Annually	1	Annually
Annually	1	Annually

The following ratings must be used for Key Controls after testing is complete:

- Satisfactory: Results indicate that the Key Control operates effectively
- Not Satisfactory: Business Issue (BI): Results indicate that the Key Control does not operate effectively and could have a negative impact on the RCSA Entity, or a significant component of the RCSA Entity.
- Not Satisfactory: Major Business Issue (MBI): Results indicate that the Key Control does not operate effectively and could have a material negative impact on the RCSA Entity, or a significant component of the RCSA Entity.

Continuing with the automobile example, the logic to decide the ratings of the controls is shown below with examples.



Corrective Action Plan (CAP) is required where the controls are found to be inadequate to mitigate the risk. A CAP should address areas of weakness identified during testing where controls are absent, inadequate or ineffective. CAPs are required when:

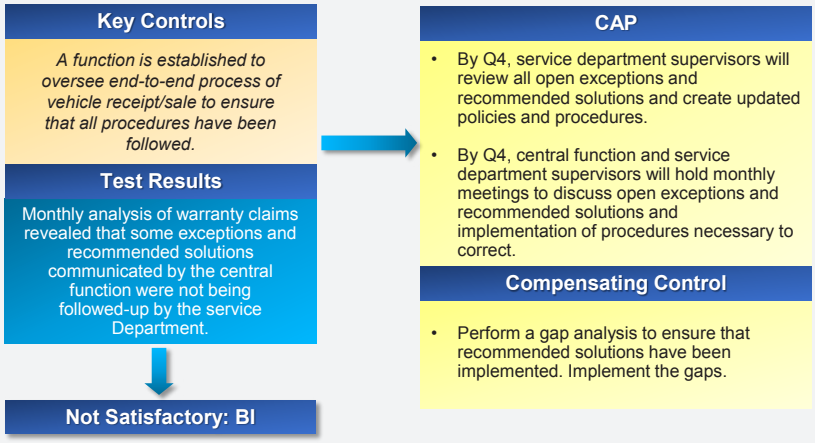
- There is a lack of a Key Control(s) against an Important Risk
- An Important Risk has not been significantly mitigated by a key control
- As a result of testing, you've concluded that the controls are not operating effectively

If the CAP cannot be implemented within the stipulated time frame, then compensating controls that mitigate the Important Risk must be identified or put in place as a temporary measure. Compensating controls must be tested until the key control that is the subject of the corrective action is implemented and tested

Everyday Example

Documenting & Defining → Identifying → Assessing & Assigning → Reviewing & Approving

- Continuing with our everyday example, let's see how a CAP has been assigned to the control issue for the Pre-owned Auto Inspection and Repair (RCSA Entity)



Each RCSA Entity must assign a Risk and Control Rating to each Important Risk on a residual basis and assessed as:

- **Acceptable:** Key Control(s) assessed as 'Satisfactory'
- **Acceptable with Concerns:** Key Control(s) assessed as 'Not Satisfactory', but compensating controls are in place to reduce the risk to an acceptable level. CAPs to be implemented can be accomplished without significantly diverting resources from business objectives
- **Less-than-Acceptable:** Key Control(s) assessed as 'Not Satisfactory', and compensating controls are not in place to reduce risk to an acceptable level.

  The rating should also be used when CAPs cannot be accomplished without significantly diverting resources from business objectives

Everyday Example

Documenting & Defining → Identifying → Assessing & Assigning → Reviewing & Approving

- Continuing with our everyday example, let's look at the Risk & Control Ratings assigned to the Important Risks that have been identified for the Pre-owned Auto Inspection and Repair (RCSA Entity)

Risk	Description	Rating
"Top-Down" Important Risk	Improper maintenance/repairs can result in car breakdowns, unreliable performance and customer dissatisfaction.	Acceptable
Regulatory Risk	The risk of non-compliance with laws regarding sale of cars with hidden defects (Lemon Law, for ex.) can result in financial loss due to warranty claims and lost customers.	Acceptable with Concerns
RCSA Entity Owner Identified Risk	The risk of selling damaged cars as "certified, pre-owned" can result in reputational damage .	Acceptable

4.4 Reviewing and Ratings

A Risk & Control Rating must be assigned to the RCSA Entity as a whole and is the responsibility of the head of the RCSA entity. The Risk & Control Rating must be Acceptable, Acceptable with Concerns, or Less-than-Acceptable. The RCSA Entity Risk & Control Rating is assigned after taking into consideration the following:

– Risk & Control Ratings of each Important Risk,

– Any other known issues, and

– Management's judgment

Thus the final rating of the RCSA entity must be based on rules like worst rating of risks or weighted average of ratings of risks with a slab definition to define risk for the entity. The processes must have the ability to provide manual override with authorization for final rating of the entity.

There must be an ability to consolidate ratings across RCSA entities to arrive at organization or enterprise based risk rating. This can also be based on rules as worst rating or a weighted average of ratings of various RCSA entities with a slab definition to define the risk of the organization or enterprise.

4.5 Key Risk Indicators

The RCSA process and Management review of business will help classifying risks by risk levels. Risks below certain risk levels can be ignored as they are not applicable to the RCSA entity or are very unlikely to occur. Risks identified as important or key risks must be monitored and reviewed through the RCSA process.

Key risks should have thresholds for escalations and if they are continuously below certain thresholds for a considerable period of time, a review must be conducted to see if it is still a key risk or not.

5. Loss Events Data

Each RCSA entity will have to capture actual loss events or incidents during the reporting period. Each loss event will have the following attributes:

- RCSA Entity code
- Incident reference number
- Description of the incident
- Key Risk category with which it is associated
- Actual or estimated loss due to the incident
- Did it have customer impact
- Was it reported externally (Police/Press)
- Potential cause of the incident
- Suggested remedy to prevent recurrence

While we can capture more descriptive or categorization data for each loss event, the key fields are the following:

- linking the incident to the right key risk category and
- Actual or estimated loss value

The above will have a key impact in computing capital charge for operational risk for the bank.

6. Reporting

Each RCSA entity will submit a periodic (defined by the bank) RCSA report. The periodicity could be different based on the nature of work done in each RCSA entity. The need for the reports/Queries given below is visualized. This section will need a review and will vary from customer to customer. We will also have to come up with some good dashboards and this can come out of a discussion once the concept is understood.

6.1 RCSA Enterprise Report

The report should contain overall rating of the organization with time period of reporting and risk rating of all RCSA entities under it. It is possible that the RCSA entities could have tiered levels and appropriate levels of drill down will have to be provided.

6.2 RCSA Entity Report

All entities will have to submit a report at the prescribed periodicity.

- Loss Events – Covered in section 5. Fields required for the report could vary from bank to bank
- RCSA results summary at entity level – overall rating, number of risks and method adopted for overall rating
- Key Risks and associated ratings with drill down to sampling tests, if required
- Management Summary – free text

6.3 Risk-Control Environment Summary report

Element	Description
Risk Reference Number	Can be sequential, used by GCRM QA team for tracking purposes (e.g. 1-1, RES.2-2 etc)
Core Process	Business process performed within a Test Unit (e.g., Change Mgmt, Info Sec, BCS, etc.). Used by GCRM QA team to facilitate communication flow for QA results to Test Units
Risk Description	Description of the specific risk applicable to the Test Unit's process
Risk Level (Important or Not Important)	Designate if the risk is “Important” or “Not Important.” If a risk is “Not Important”, then a rationale must be documented
Control Reference Number	Can be sequential, used by GCRM QA team for tracking purposes
Control Description	Description of controls in place for a given process in a Test Unit. These controls mitigate Important Risks.
Control Level	Indicate if the control is a key control

6.4 Risk Control Testing Details

Element	Description
Test Points	Customized test steps identified to test the effectiveness of a given control
Testing Frequency	Indicate the testing frequency of the control (e.g., quarterly, semi-annually, annually). Testing frequency is how often that control process is tested and documented in the RCSA.
Sample Size	Provide sample size, as per the new minimum test frequencies as defined in the RCSA Policy ("RCSA Minimum Sample Size Table” in Appendix I)
Location of Supporting Evidence	Provide description of where documentation supporting testing is maintained, i.e., exactly align/ map each test point with the sample evidence location. This alignment / mapping is critical for the GCRM QA process
Summary of Test Results	Indicate the results of testing, including a detailed summary of the findings. Test results should be aligned to the test steps
Control Assessment (Operating Effectiveness)	Identify whether the control is operating effectively. Rate as Satisfactory, Not Satisfactory (Business Issue) or Not Satisfactory (Major Business Issue)
Risk & Control Rating (Residual)	Assign a Risk & Control Rating to each Important Risk on a residual basis, i.e., after consideration of the control testing results. Rate as Acceptable, Acceptable with Concerns or Less-than-Acceptable
Description of the Deficiency and Control Issue #	Provide a description of the control weakness detected during testing. Provide the target date for completion and ID # that corresponds to the Control Issue. If an ID # has not been assigned then state TBD

7. Capital Computation

The capital computation for operational risk is based on:

- Internal Loss Data
- External Loss Data

Internal Loss data is captured by the bank and external loss data can be used and supplementary data where internal data is not found adequate. It is the bank's responsibility to arrange and collect external data.

There are three methods for computing capital charge:

- Loss Distribution Approach (LDA)
- Scenario Based AMA
- Risk Drivers and Control Approach

Under LDA, Capital is computed using Model loss distributions obtained by fitting Internal and/or external loss data. Capital is obtained from a joint frequency/severity distribution.

Under Scenario based approach, a large number of discrete loss scenarios are identified and quantified (from a combination of loss data and expert judgment). "A bank must use Scenario Analysis of expert opinion in conjunction with external data to evaluate its exposure to high severity events. This approach draws on the knowledge of experienced business managers and risk management experts to derive reasoned assessments of plausible severe losses. Scenario Analysis involves identifying plausible future events and making educated assumptions to generate "what if" scenarios and examine their possible impact on our businesses. Scenario Analysis can help management make contingency plans to

- reduce the impact from such scenarios, and
- implement or strengthen controls to reduce the likelihood of scenarios happening

Scenario Analysis will be an additional tool for both the measurement and management of Operational Risk.

Under Risk Drivers and Control Approach, capital is posted using BIA approach (or standardized approach) and allocated to units based on risk drivers. Relationship between capital and risk drivers can be done using an algorithm based on loss data or risk control ratings – there is nothing fixed and it can vary from bank to bank.

In this document, we will focus on computing capital charge using Scenario based Approach. The following steps should be used to compute the capital charge:

- Compute average loss associated with each loss event. The weightage given to external and internal data can be different.
- Based on frequency of occurrence over a period of time (say 3 years), compute the probability of occurrence of the event.
- Check the RCSA rating for the risk associated with the loss event. Associate a premium on capital charge, if the risk rating is "Acceptable with Concerns" or "Less than Acceptable"
- The bank can specify a minimum capital charge for risks which do not have loss events.
- Compute estimated losses for scenarios painted by the expert and associate a probability with the likelihood of the scenario. Multiply the two to arrive at a scenario premium in additional to the actual loss based capital charge
- The summation of actual loss charge and scenario based charge will become the operational risk capital charge.

Some banks may want to compare the operational risk charge computed by above methodology and the BIA approach and take the higher of the two till processes stabilize.

The capital charge for operations risk can be a sum of (average loss* Probability of occurrence*weightage for external/internal*risk rating factor based on rating) across all risks.

8. Annexure

Process				Risk			Control Activities	
	Process		Sub-process		Specific Risk	Inherent Risk Level		Control Activity
1	Compliance	1.1	US compliance	1.1.1	Businesses do not comply with US regulatory requirements			
		1.2	Host country compliance	1.2.1	Businesses do not comply with host country regulatory requirements (regulatory definitions and accounting differences)			
				1.2.2	Not all legal vehicles that require regiulatory reporting are covered.			
				1.2.3	Insufficient knowledge and training is provided to resources to establish Basel II expertise			
		1.3	Bank compliance	1.3.1	Businesses do not comply with Bank Basel II policies and procedures			
				1.3.2	Exceptions to Bank policies, procedures and standards are not approved and signed-off			
2	Exposure identification & segmentation	2.1	Exposure identification & classification	2.1.1	Incomplete identification of all Basel II exposure			
				2.1.2	New products / business lines are not addressed under the Basel II requirements framework			
				2.1.3	Inaccurate definition of exposures to Basel II categories (Retail, Wholesale, Equity, Financial Instruments and Securtization)			
				2.1.4	Migration of exposures between segments is not covered			
		2.2	Exposure segmentation	2.2.1	Incorrect segmentation of retail exposures into sub-categories			
				2.2.2	Inconsistent segmentation of retail exposures over time			
		2.3	Scoring	2.3.1	Unapproved Basel II scores are used for segmentation			
				2.3.2	Inconsistent use of scores in supplemental segmentation			
				2.3.3	Not all scored accounts are used in the suplemental score segmentation			
		2.4	Exposure pooling	2.4.1	Incorrect pooling of Basel II retail exposures			
				2.4.2	Exposures are not pooled according to latest business requirements			
				2.4.3	Not all accounts are covered in the exposure pooling process			
		2.5	Documentation	2.5.1	Incomplete documentation of exposure identification & segmentation processes and procedures			
3	Data submission	3.1	Monthly portfolio data submission	3.1.1	Incomplete monthly data submission of all Basel II exposure categorues (Retail, Wholesale, Equity, Financial Instruments and Securtization)			
				3.1.2	Incomplete monthly data submission of financial decomposition files			
				3.1.3	Basel II data submissions are not submitted in a timely manner (considering initial submissions and potential resubmissions due to data quality issues)			
				3.1.4	Basel II submissions are rejected due to non-compliance with requirements			
				3.1.5	Unapproved simplified portfolios			
				3.1.6	Coverage of standard submission portfolios is too low			
		3.2	Business owbership	3.2.1	Basel II data submissions are not signed off in a timely manner			
				3.2.2	Risk Parameters and RWA results are not reviewed and approved by businesses			
				3.2.3	Businesses do not comply with the regulatory 'use test' requirements			
		3.3	COB	3.3.1	A COB is not in place or does not cover Basel II			
4	Data Quality	4.1	Data Formatting	4.1.1	Incorrect formatting of Basel II data submissions			
		4.2	Data Integrity	4.2.1	Logical errors / breaks exist in the Basel II data submissions			
				4.2.2	Not all data elements requested are available and provided			
				4.2.3	Data and submisison exceptions have not been approved and signed off			
				4.2.4	Incorrect data submisions and data integrity issues are not addressed in a timely and complete manner			
				4.2.5	No local data quality checks are performed to ensure highest data quality			
				4.2.6	Basel II data submissions are not reconcilied			
				4.2.7	Reconciliation differences are not explained / tracked			
5	Data Managament and Maintenance	5.1	Storage	5.1.1	Not enough historical data is stored for regulatory review (Basel II requires 5+ years of account level data, pooling code and pooled data submissions)			
				5.1.2	Basel II submissions are not properly secured in storage according to their classification (records management)			
		5.2	Transmission	5.2.1	Basel II submissions are not properly secured during transmission according to their classification			
		5.3	Entitlement	5.3.1	Basel II submisions are not properly secured through entitlements during data extract and preparation			
				5.3.2	Basel II information is not properly secured through entitlements in the GCBC system			
		5.4	Cross border compliance & privacy	5.4.1	Data submissions do not comply with local cross border standards and regulations			
				5.4.2	Data submissions do not comply with local data pricavy standards and regulations			

About the Author:

Ravi Raman is Chief Solutions Evangelist at iCreate Software and is a senior Basel II/III specialist. Ravi has been associated with IT industry for 33 years and has worked in diverse roles across companies. He has successfully implemented over 100 projects and managed large software development units and data centres spread across 30 countries. He has spent 25 of the 32 years with Citigroup in various capacities. Previously, Ravi held leadership positions at Tata Burroughs Limited, International Data Management and was CEO of Duncans and Hexaware. He is well-versed with the entire spectrum of Banking Technology across Corporate Banking, Risk Management, MIS, Regulatory Reporting and Infrastructure Management. His areas of specialization are Basel II/III and DW for Banks.

iCreate Software Pvt. Ltd.
5 - 10, Guava Garden, 17 H Main, 5th Block, Koramangala, Bangalore 560 095.
T: +91 80 405 89 400 E: info@icreate.in W: www.icreate.in